

CopyV2H(A7,TS1)
CopyH2H(B7,TC1)

																								P8		n(x)		P7		P6		P5		P4		n(x)		P3		P2		n(x)		P1		P0							
X8	X7	X6	X5	X4	X3	X2	X1	E8	E7	E6	E5	E4	E3	E2	E1	A8	A7	A6	A5	A4	A3	A2	A1																														
																								TS8	TS7	TS6	TS5	TS4	TS3	TS2	TS1	TS0											TS8	TS7	TS6	TS5	TS4	TS3	TS2	TS1	TS0		
																								TC8	TC7	TC6	TC5	TC4	TC3	TC2	TC1	TC0											TC8	TC7	TC6	TC5	TC4	TC3	TC2	TC1	TC0		
23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0																														

ModAdd(TS1,TC1)

ModAdd(TS1,TC1)
CopyH2V(B1,A7)

X2	Y2	Z3	X1	Y1	Z1	A(P)	B(P)	T8	I	H	EXP	B8	T7	B7	E	B6	E	B5	B4	G	B3	B2	I	B1	0		
													n(x)		6	n(x)		n(x)		n(x)		n(x)		n(x)		n(x)	
													P8	P7	P6	P5	P4	P3	P2	P1	P0						
X8	X7	X6	X5	X4	X3	X2	X1	E8	E7	E6	E5	E4	E3	E2	E1	A8	A7	A6	A5	A4	A3	A2	A1				
													TS8	TS7	TS6	TS5	TS4	TS3	TS2	TS1	TS0						
													TC8	TC7	TC6	TC5	TC4	TC3	TC2	TC1	TC0						
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*E*rinvpoly
CopyH2V(B5,A7)
CopyH2H(B5,B7)
MontMult(A7,B7,P1)

T10 = T9*E*invpoly																								
X8	X7	X6	X5	X4	X3	X2	X1	E8	E7	E6	E5	E4	E3	E2	E1	A8	A7	A6	A5	A4	A3	A2	A1	

T10 = T9*E*rinvpoly
MontMult(A7,B7,P1)

X2		Y2	Z3	X1	Y1	Z1	A(P)	B(P)	E	I	H	EXP	B8	T10	B7	B6	E	B5	B4	G	B3	B2	T8	B1	0	
X8	X7	X6	X5	X4	X3	X2	X1	E8	E7	E6	E5	E4	E3	E2	E1	A8	A7	A6	A5	A4	A3	A2	A1			
		P8	n(x)		P7	P6	n(x)		P5	P4	n(x)		P3	P2	n(x)		P1	P0	n(x)		P1	P0	n(x)		P1	P0
		TS8	TS7		TS6	TS5		TS4	TS3		TS2	TS1		TS0	TS2		TS1	TS0	TS2		TS1	TS0	TS2		TS1	TS0
		TC8	TC7		TC6	TC5		TC4	TC3		TC2	TC1		TC0	TC2		TC1	TC0	TC2		TC1	TC0	TC2		TC1	TC0
23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0			

X3 = T8-T10
CopyH2H(B1,TS1)
CopyH2H(B7,TC1)

CopyH2H(B1,TS1) CopyH2H(B7,TC1)																																													
X2	Y2	Z3	X1	Y1	Z1	A(P)	B(P)	E	I	H	EXP	T10			E			G			T8																								
X8	X7	X6	X5	X4	X3	X2	X1	E8	E7	E6	E5	E4	E3	E2	E1	A8	A7	A6	A5	A4	A3	A2	A1	B8	B7	B6	B5	B4	B3	B2	B1	0													
																								n(x)			n(x)			n(x)			n(x)												
																								P8	P7	P6	P5	P4	P3	P2	P1	P0													
												TS8	TS7	TS6	TS5	TS4	TS3	TS2	TS1	TS0																									
												33	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0

ModAdd(TS1,TC1)
CopyH2V(B1,X7)

ModAdd(TS1.TC1)																								
CopyH2V(B1.X7)																								
X3	Y2	Z3	X1	Y1	Z1	A(P)	B(P)	E	I	H	EXP	B8	T10	B7	B6	E	B5	B4	G	B3	B2	X3	B1	0
													n(x)	P7	P6	n(x)	P5	P4	n(x)	P3	P2	n(x)	P1	P0

T11 = I*X3*rinvpoly
CopyV2H(A5,B1)
MontMult(X7,B1,P1)
CopyH2V(B1,A7)
CopyH2H(B1,B7)

CopyVZ(H(A5,B1)																											
MontMult(X(7,B1,P1)																											
CopyH2(V(B1,A7)																											
CopyZ2(H(B1,B7)																											
X3	Y2	Z3	X1	Y1	Z1	A(P)	B(P)	I	I	H	EXP	T11		E		G		X3									
												B8	B7	B6	B5	B4	B3	B2	B1	0							
												n(x)		n(x)		n(x)		n(x)		n(x)							
X8	X7	X6	X5	X4	X3	X2	X1	E8	E7	E6	E5	E4	E3	E2	E1	A8	A7	A6	A5	A4	A3	A2	A1				
												P8	P7	P6	P5	P4	P3	P2	P1	P0							
												15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0

T12 = G*G*rinvpoly
CopyH2V(B3,A7)
MontMult(A7,B3,P1)

MonteMitt(A,B5,P1)																								
X3		Y2	Z3	X1	Y1	Z1	A(P)	B(P)	T11				E				T12				X3			
									G	I	H	EXP	B8	B7	B6	B5	B4	B3	B2	B1	0			
									11				n(x)							n(x)				
X8	X7	X6	X5	X4	X3	X2	X1	E8	E7	E6	E5	E4	E3	E2	E1	A8	A7	A6	A5	A4	A3	A2	A1	
		P8	n(x)		P7	P6	n(x)		P5	P4	n(x)		P3	P2	n(x)		P1	P0	n(x)		P1	P0		
		T8	TS7		T7	T6	TS6		T5	T4	TS3		T2	T1	TS2		T0	T0	TS2		T1	T0		
		TC8	TC7		TC6	TC5	TC4		TC3	TC2	TC1		TC0	TC0	TC2		TC1	TC0	TC2		TC1	TC0		
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 = T12*H*rinvpoly
CopyH2H(B7,TS1)
CopyH2H(B3,TC1)

X3		Y2	Z3	X1	Y1	Z1	A(P)	B(P)	G	I	H	EXP	B8	T11	B7	B6	E	B5	B4	T13	B3	B2	X3	B1	0							
													7		n(x)		n(x)		n(x)		n(x)											
													P8		P7		P6		P5		P4		P3		P2		P1		P0			
													T8		TS7		T7		TS6		T5		TS4		T3		TS2		T1		TS0	
													TC8		TC7		TC6		TC5		TC4		TC3		TC2		TC1		TC0			
23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0									

ModAdd(TS1,TC1)
CopyH2V(B1,X5)

X3
