- *// ring var: RATO, all bit-level inputs (PS and PI) followed by P, S and T*
- ring rr = (2,X), (n23,n43,n42,n18,n40,n39,...<omitted bit-level intermediate vars>...,**x0,x1,s0,s1,s2,s3,P,S,T**), lp;
- minpoly = X^4+X+1;

- ideal A_in = s0,s1,s2,s3;
- poly **def_S** = s0+s1*X+s2*X^2+s3*X^3+S;
- ideal X_in = x0,x1;
- poly **def_X** = x0 + x1*X^5+P;
- poly red_S = S^16+S; *// GF(2^4)*
- poly red_T = T^16+T;
- poly red_X = P^4+P; *// GF(2^2) as a subset field of GF(2^4)*
- *// red_all: vanishing polys*
- ideal red_all = x0^2+x0, x1^2+x1, s0^2+s0, s1^2+s1, s2^2+s2, s3^2+s3,red_S,red_X;
- poly tran = T+(X^2+X+1)*x0*x1*s1*s3+(X^3+X)*x0*x1*s1+...<omitted>...;

- poly **init_S** = S+X^2;
- poly reached = T+X^2;

- *// Bit-word substitution*
- ideal I1 = preprocess(def_S, red_all, A_in);
- poly unitran = conv_word(tran,I1);
- I1 = preprocess(def_X, red_all, X_in);
- unitran = conv_word(unitran,I1);

- *// Iterative BFS traversal*
- int i = 1;
- ideal from_I,to_I,new_I;
- from_I[1] = init_S;
- while(1)
- {
- 	i++;
- 	to_I[i] = **transition(from_I[i-1],unitran,red_all)**;
- 	"Iteration #",i-2;
- 	"Next State(s): ",to_I[i];
- 	new_I[i] = redWord(**to_I[i]+compl(reached,red_T)**, red_T);
- 	"Newly reached states: ",new_I[i];
- 	if ((redWord(new_I[i],red_T) == 1) or (i>MAX_iter))
- 	{
- 		"**************** TERMINATE! ****************";
- 		break;
- 	}
- 	reached = redWord(**reached * new_I[i]**,red_T);
- 	"Currently reached states: ",reached;
- 	from_I[i] = subst(new_I[i],T,S);
- }
- "BFS depth: ",i-2;
- "Final reachable states: ",reached;