A Equation Construction

Figure 1 shows the equation systems derived from our method. C and x_i indicate the positions of constant and variable introduction, respectively. The red line indicates the base position, and the meeting green arrows indicate equation establishment. Equations are derived from branch expression equality, with the degree indicated by the adjacent green number, representing the higher branch degree.

Table 1: Complexity of Gröbner basis attack on Griffin.

r	2			3			4			5			6		
	n_v	$\sum equ$	cmp.	n_v	$\sum equ$	cmp.	n_v	$\sum equ$	cmp.	n_v	$\sum equ$	cmp.	n_v	$\sum equ$	cmp.
This	**2**	**20**	**15.43**	**3**	**41**	**26.97**	4	86	42.17	5	125	55.73	6	146	67.11
	3	15	18.26	4	30	29.88	**5**	**45**	**40.77**	**6**	**66**	**53.14**	**7**	**95**	**66.94**
	4	14	20.83	5	27	33.17	6	42	45.08	7	57	56.33	8	72	67.29
Griffin	7	19	21.49	10	28	32.92	13	37	44.62	16	46	56.33	19	55	68.08
	3	56	15.56	4	399	29.88	5	2.8e3	50.12	6	1.9e4	76.36	7	1.4e5	68.64

B Griffin alpha=3

Table 1 presents the results for Griffin-π with S-box degree $\alpha = 3$ for different branch numbers.

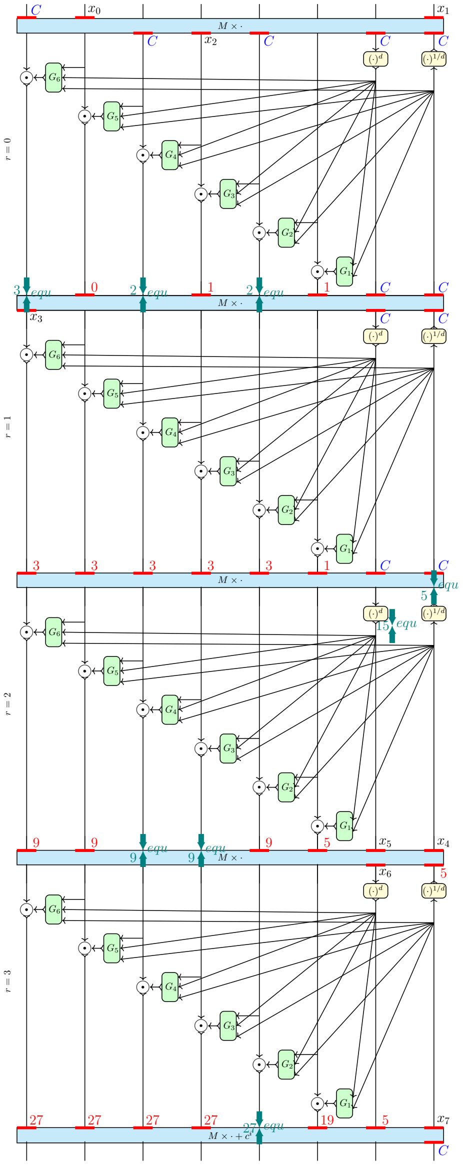

Fig. 1: Griffin: 4-round 8-branch system