

FIG. 1 Odd-even periodic extension of the rescaled sigmoid

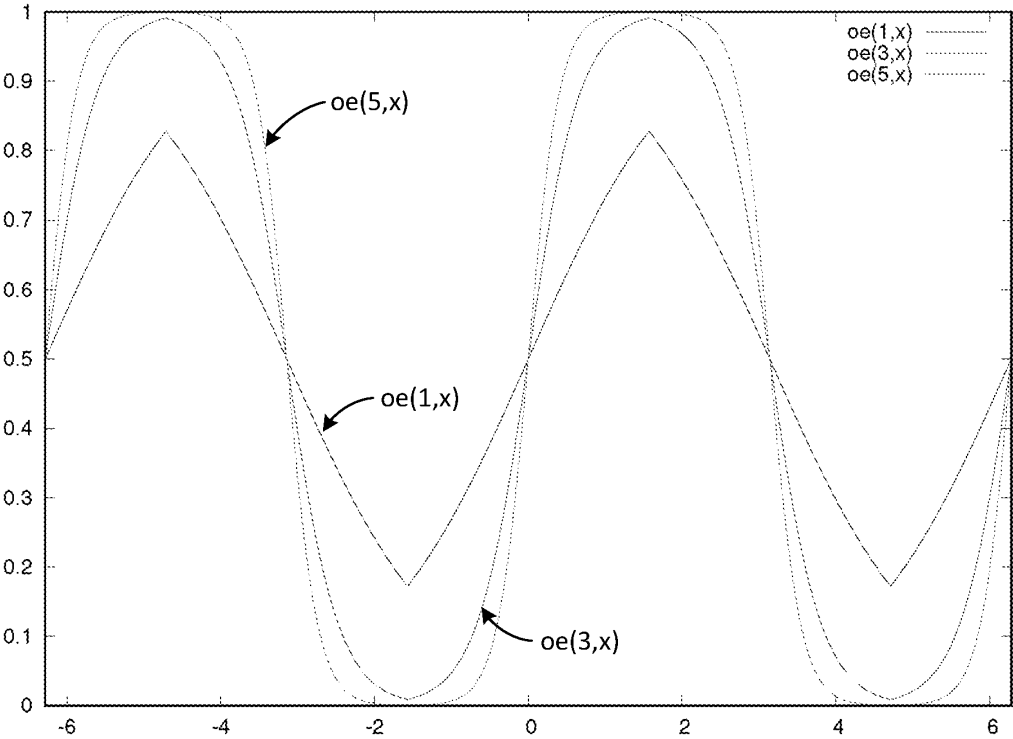


FIG. 2 Asymptotic approximation of the sigmoid via Theorem 1

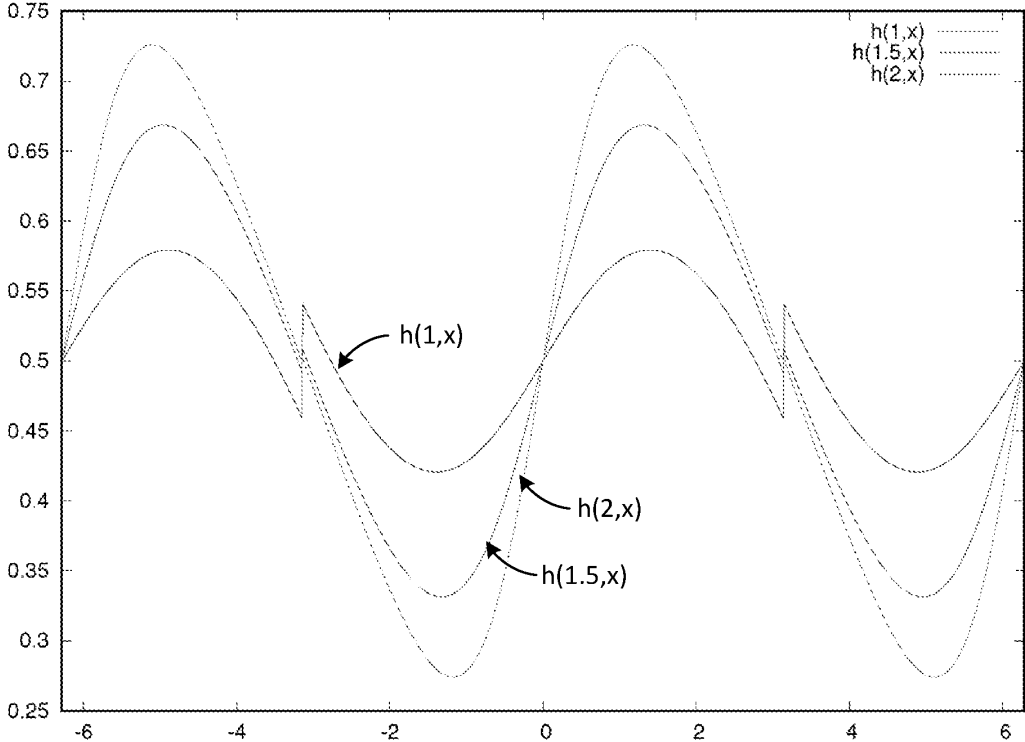
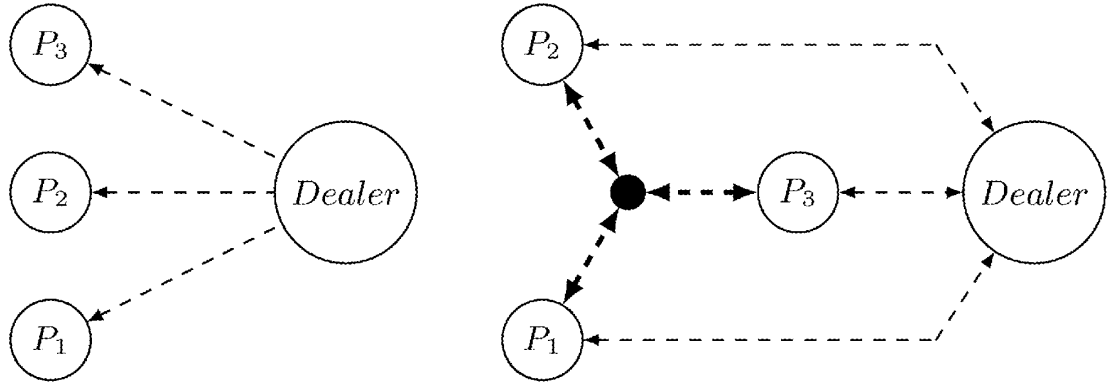
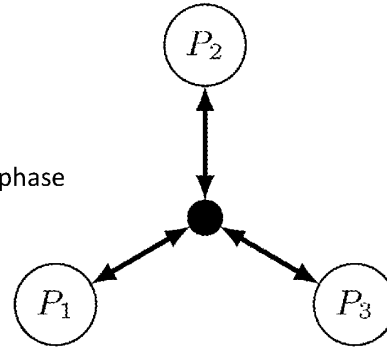


FIG. 3 Communication channels in the offline phase**FIG. 4**

Communication channels in the online phase

**FIG. 5** Experimental results for $n = 3$ players

Dataset size N	# features k	communication size (MB)	Precomputed data size (MB)	Time (sec) offline phase	Time (sec) online phase
10000	8	13.75	50.55	20.07	6.51
10000	12	21.88	66.18	26.6	9.81
10000	20	45.97	113.1	46.26	19.83
25000	8	34.2	126.23	51.59	19.24
25000	12	54.52	165.14	68.14	24.7
25000	20	114.5	281.98	115.56	48.8
50000	8	68.53	252.35	103.41	32.89
50000	12	108.93	330.1	135.07	49.99
50000	20	228.7	563.46	229.17	103.3
100000	8	137	504.6	205.53	67.11
100000	12	217.75	659.96	269.04	99.99
100000	20	457.1	1126.41	457.33	205.28
150000	8	205.48	756.84	308.14	101.36
150000	12	326.56	989.83	343.86	152.41
150000	20	685.51	1689.36	685.74	314.4

FIG. 6 Evolution of the cost function depending on the method

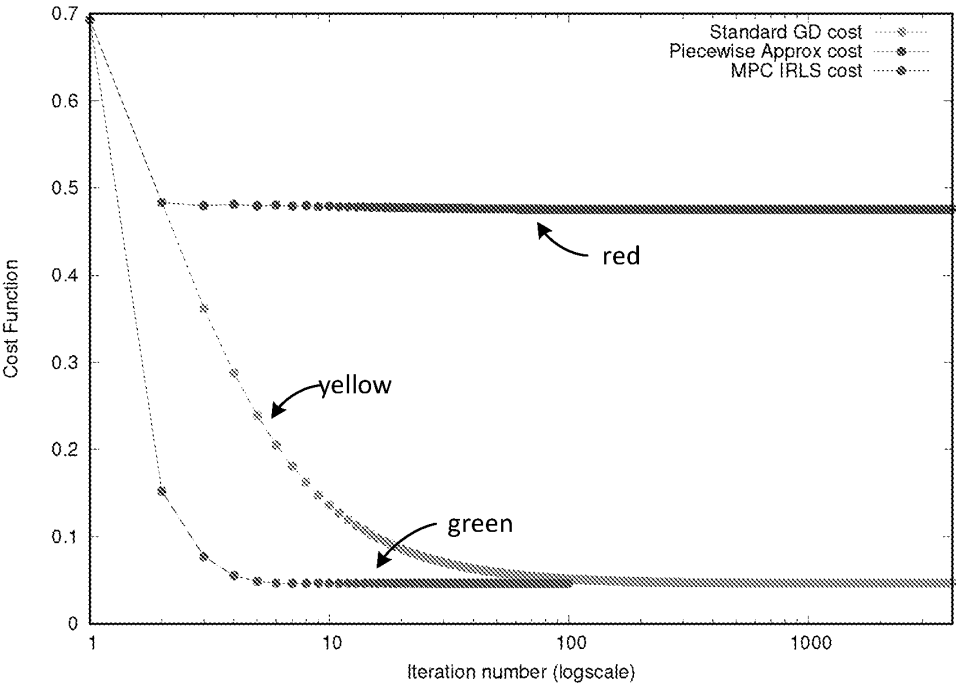


FIG. 7 Evolution of the F-score depending on the method

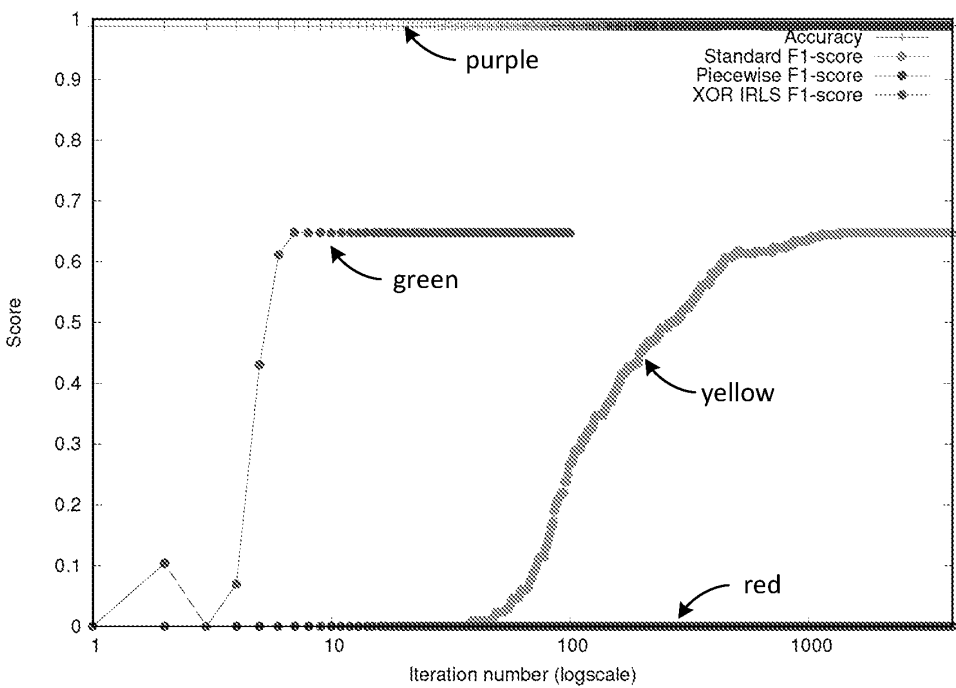


FIG. 8

The truth table of an AND gate

a	b	c
0	0	0
0	1	0
1	0	0
1	1	1

The encrypted truth table

$\text{Enc}_{K_0^a K_0^b}(K_0^c)$
$\text{Enc}_{K_0^a K_1^b}(K_0^c)$
$\text{Enc}_{K_1^a K_0^b}(K_0^c)$
$\text{Enc}_{K_1^a K_1^b}(K_1^c)$

FIG. 9

Method	Secret gate	AND	XOR
Naive	(4,4,4)	(4,4,4)	(4,4,4)
Point-Perm	(4,4,1)	(4,4,1)	(4,4,1)
PP, RR	(4,3,1)	(4,3,1)	(4,3,1)
PP, RR, free-X	(4,3,1)	(4,3,1)	(0,0,0)
PP, RR, free-X, half-Gate	N.A.	(4,2,2) private (2,1,1) known plaintext	(0,0,0)

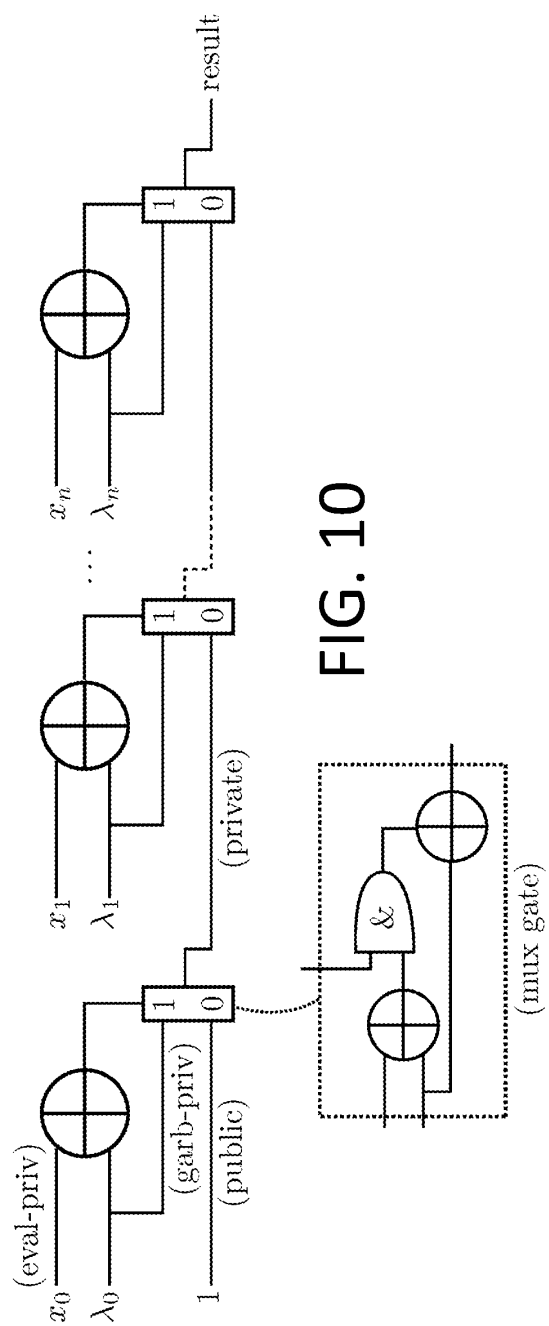


FIG. 10

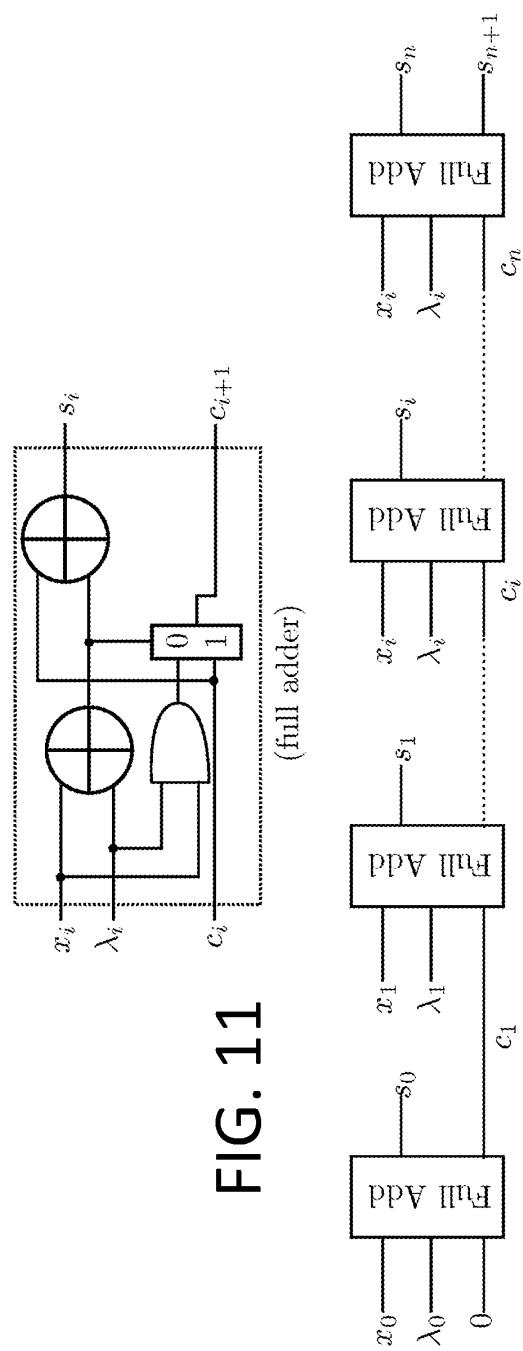


FIG. 11

FIG. 12

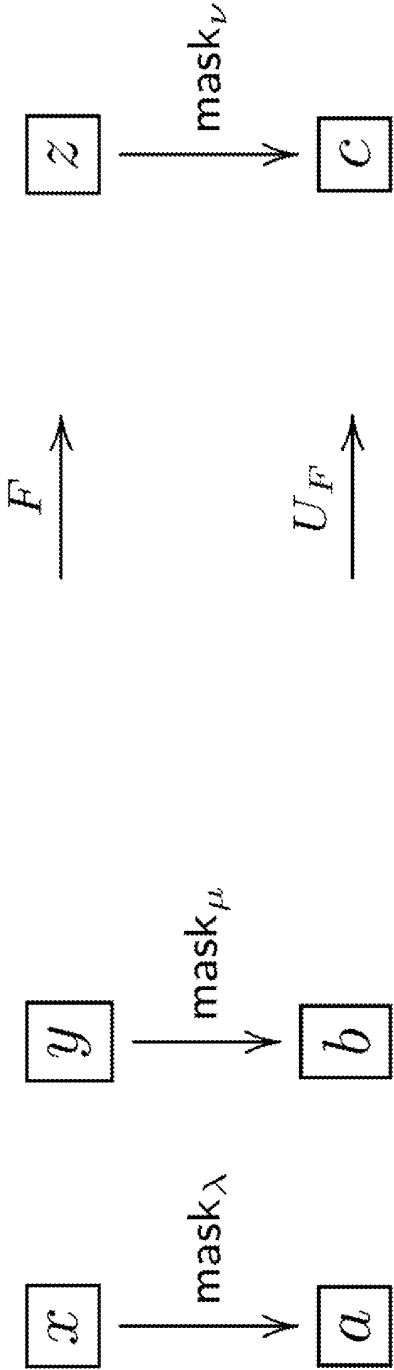
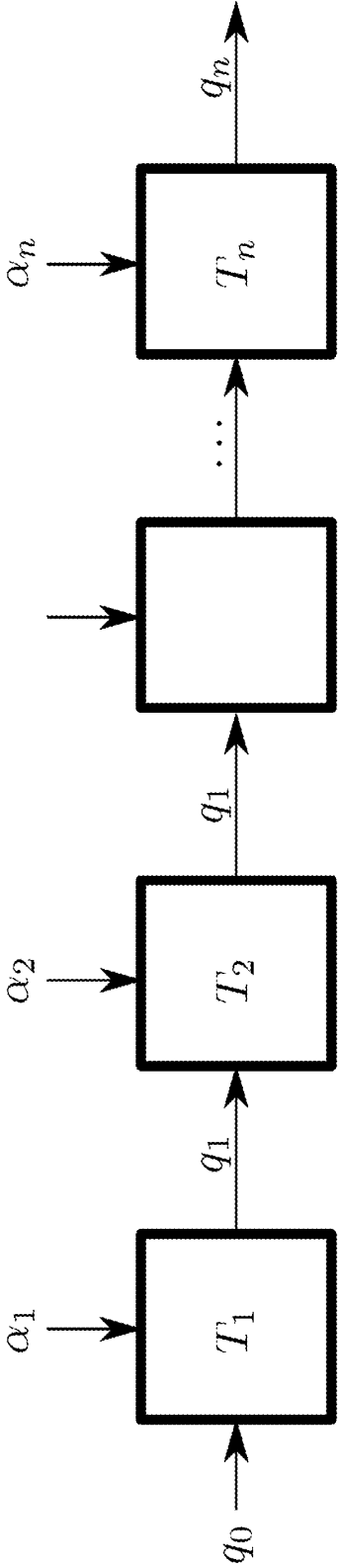


FIG. 13



7 / 9

FIG. 14

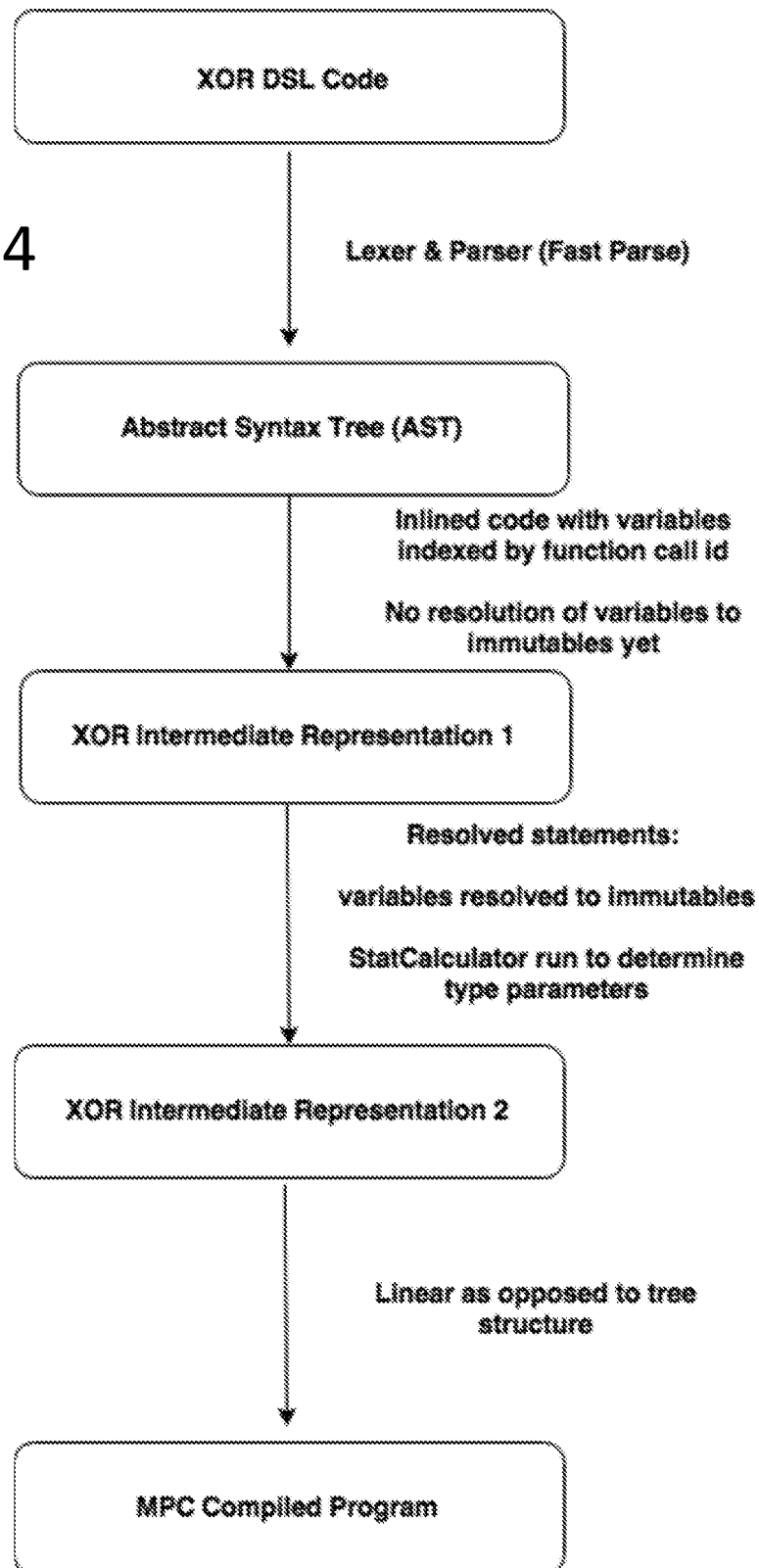


FIG. 15

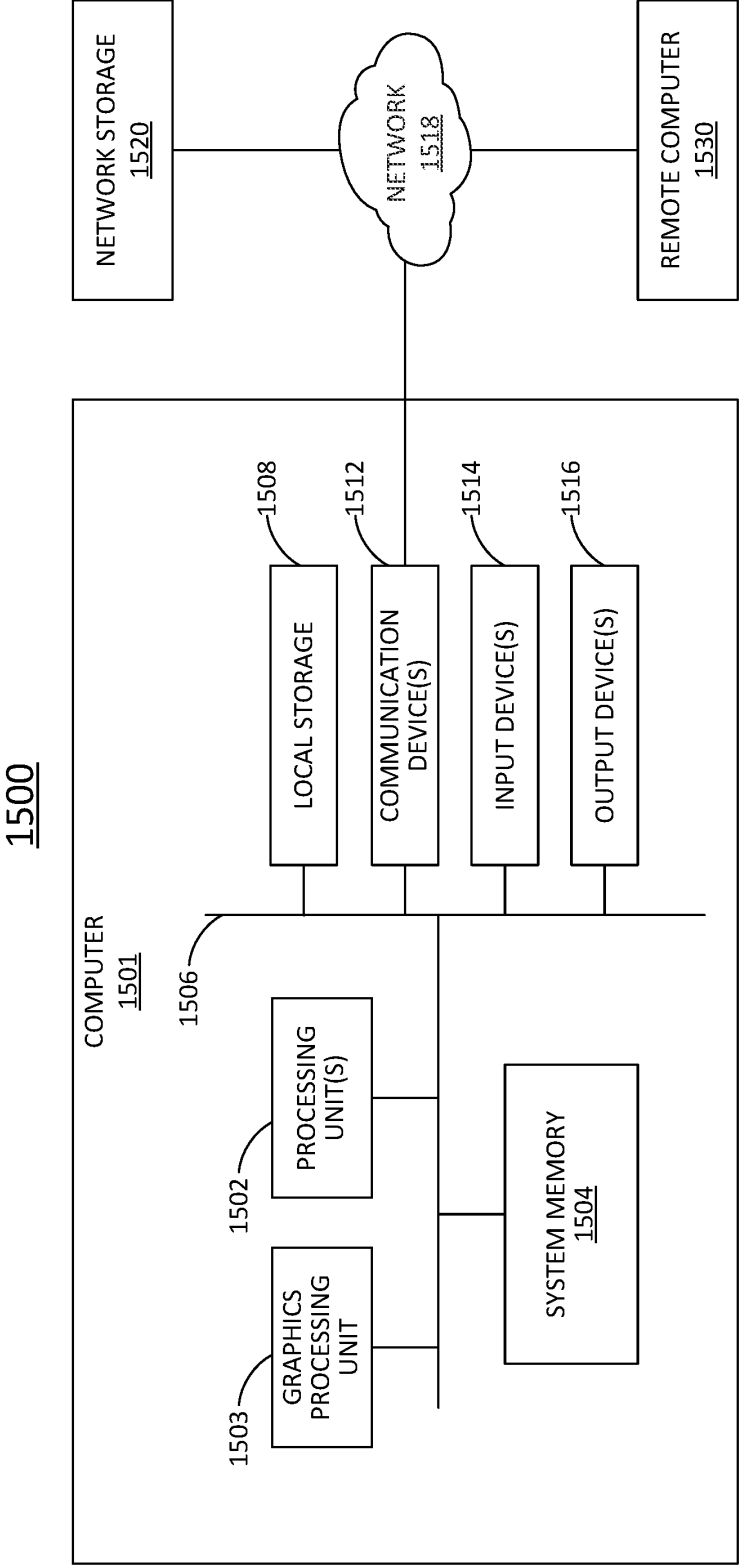


FIG. 16

