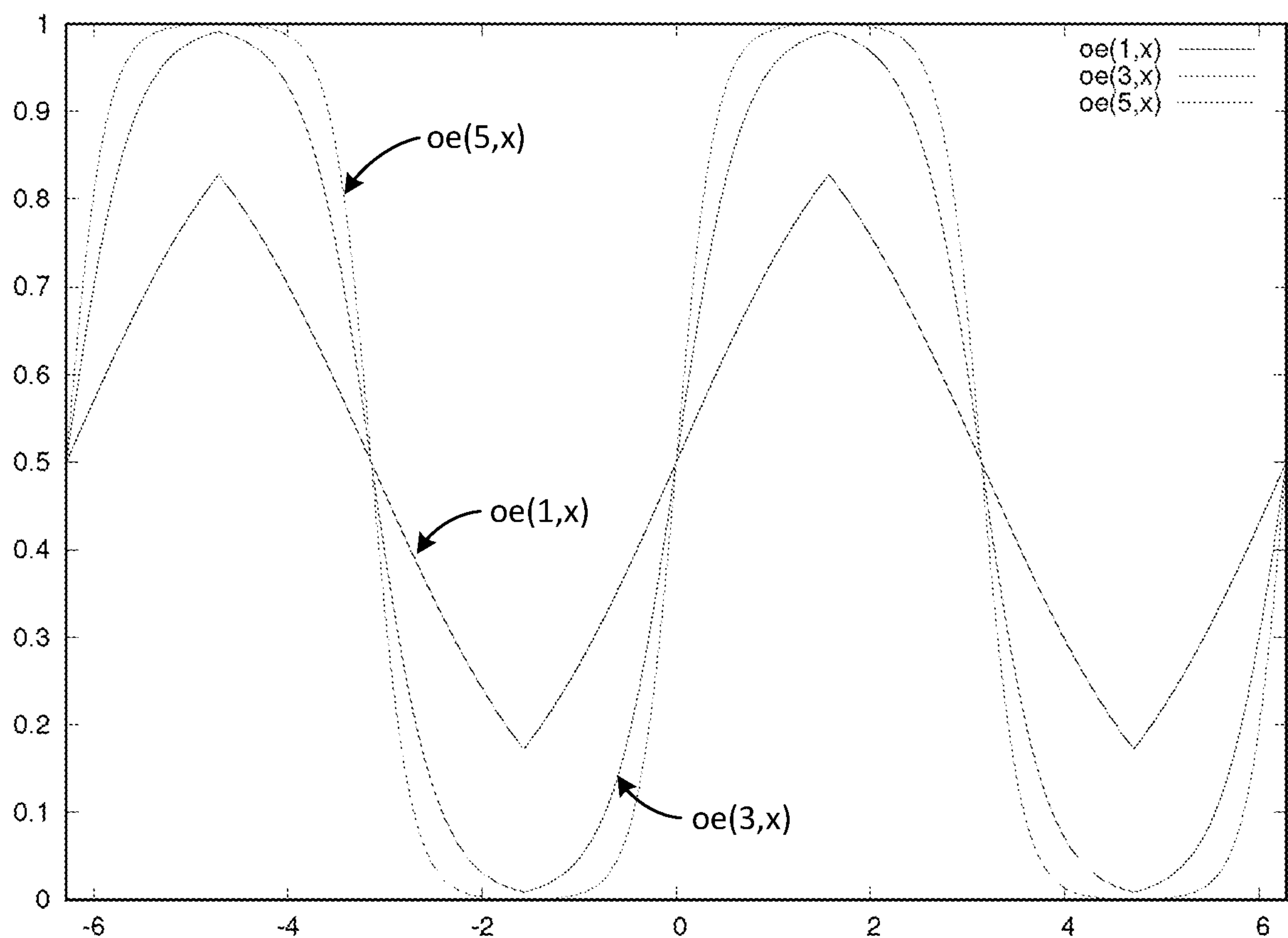


FIG. 1

Odd-even periodic extension of the rescaled sigmoid

**FIG. 2**

Asymptotic approximation of the sigmoid via Theorem 1

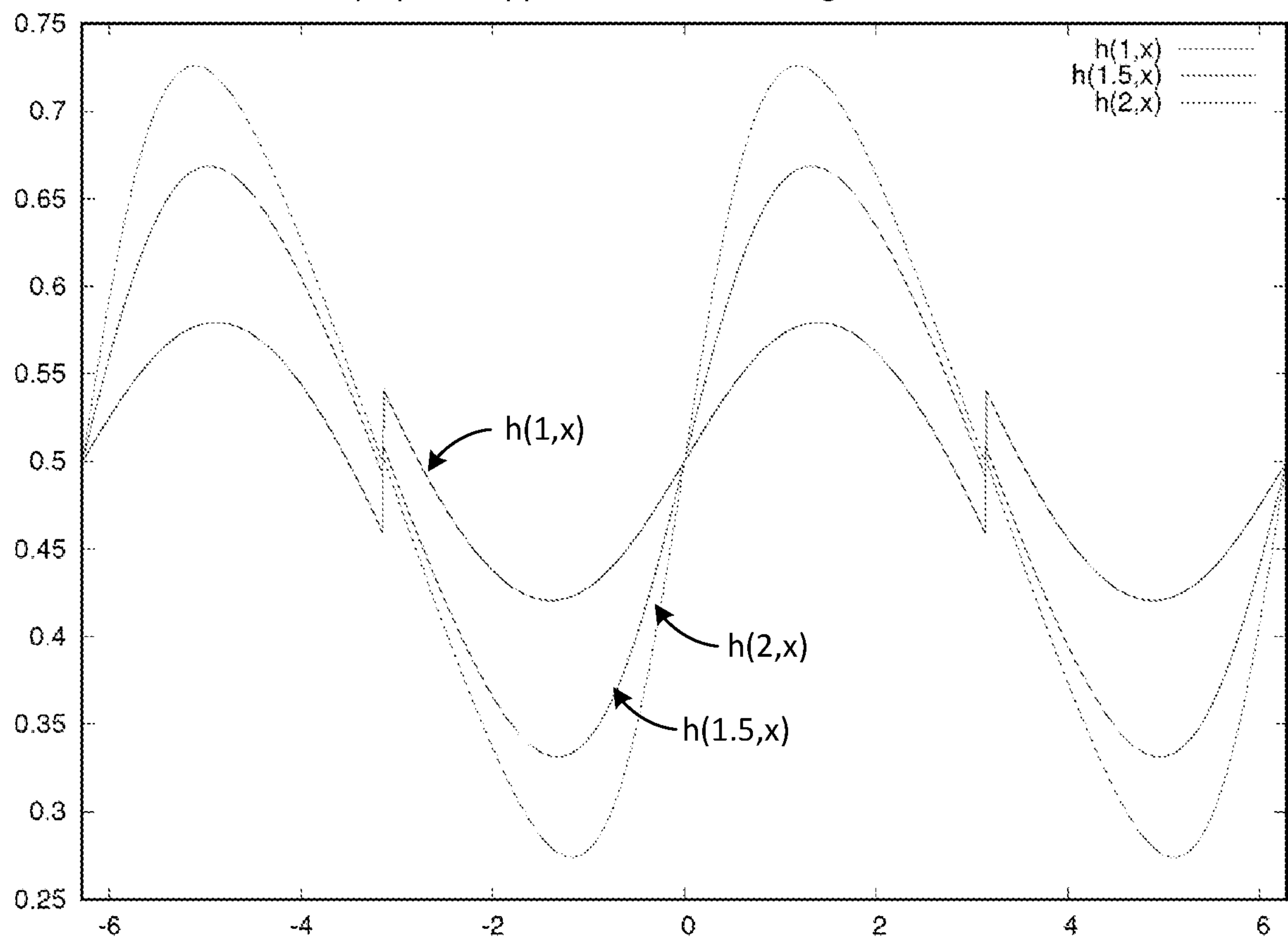
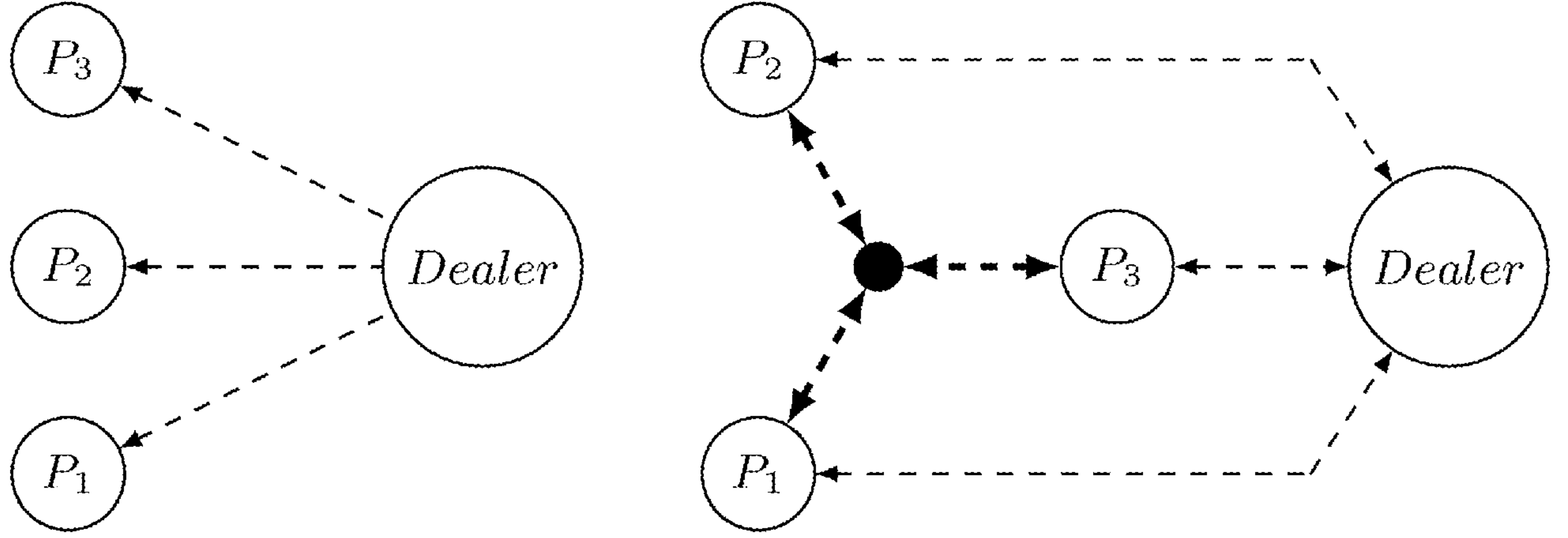
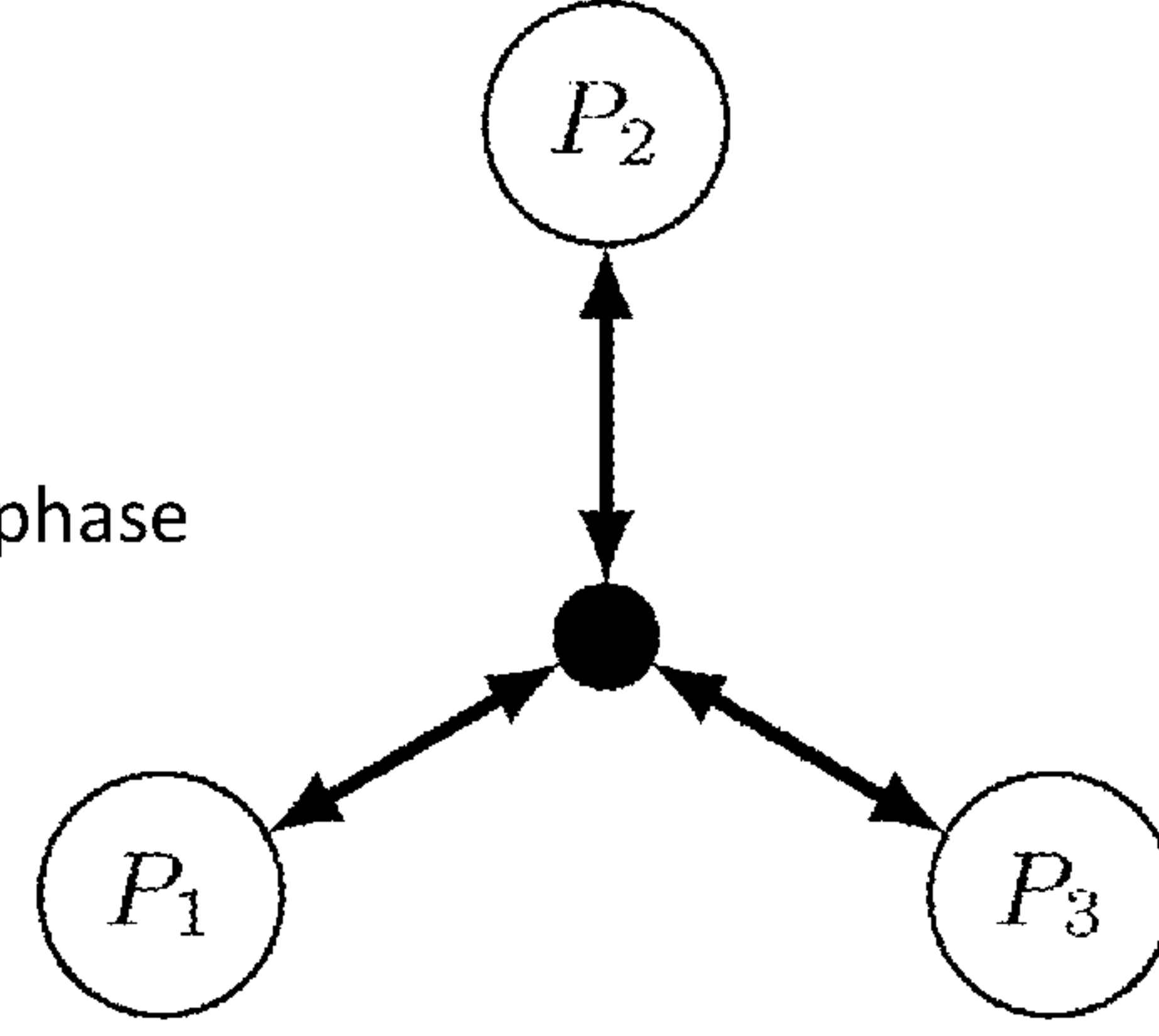


FIG. 3 Communication channels in the offline phase**FIG. 4**

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

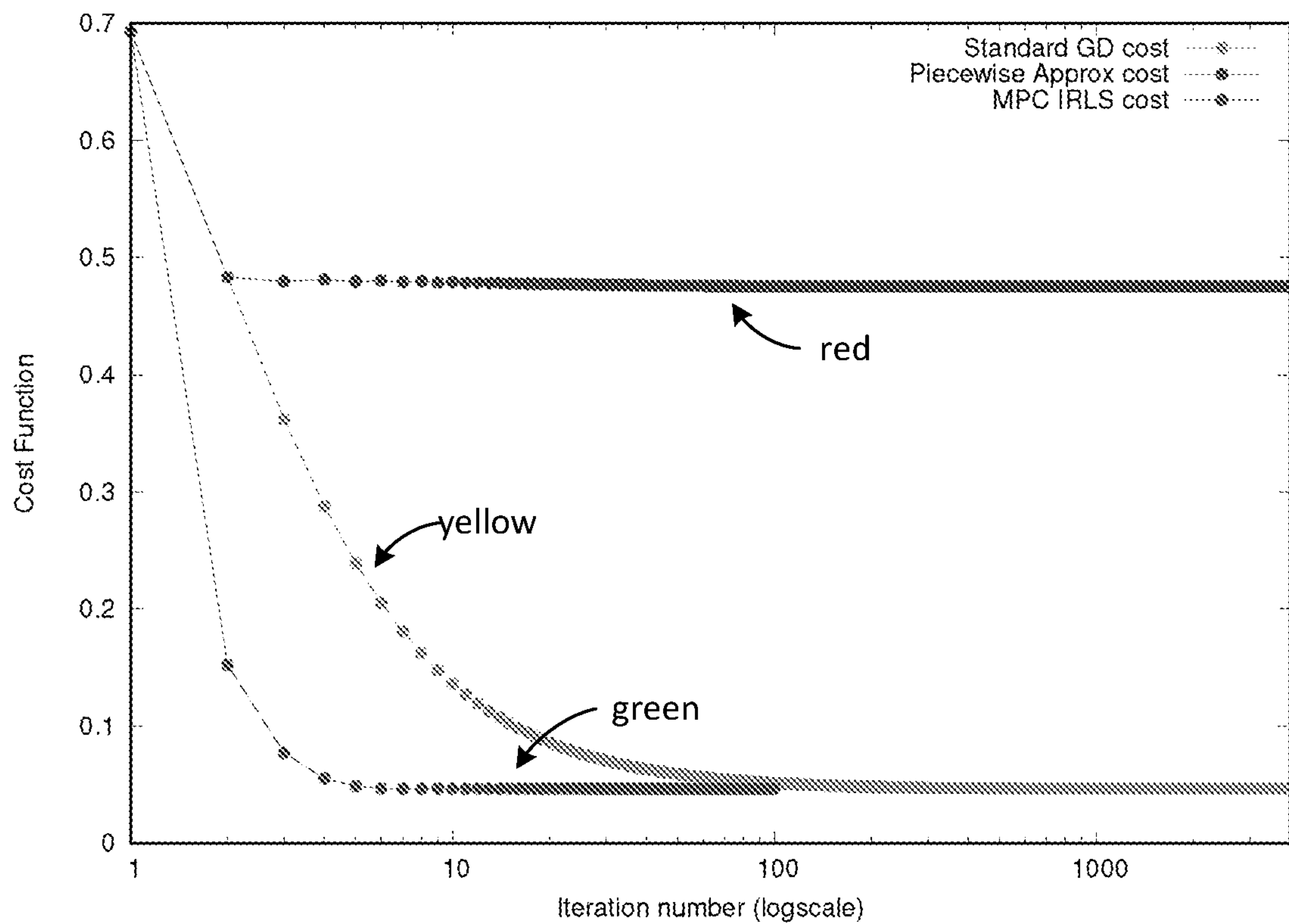


FIG. 7 Evolution of the F-score depending on the method

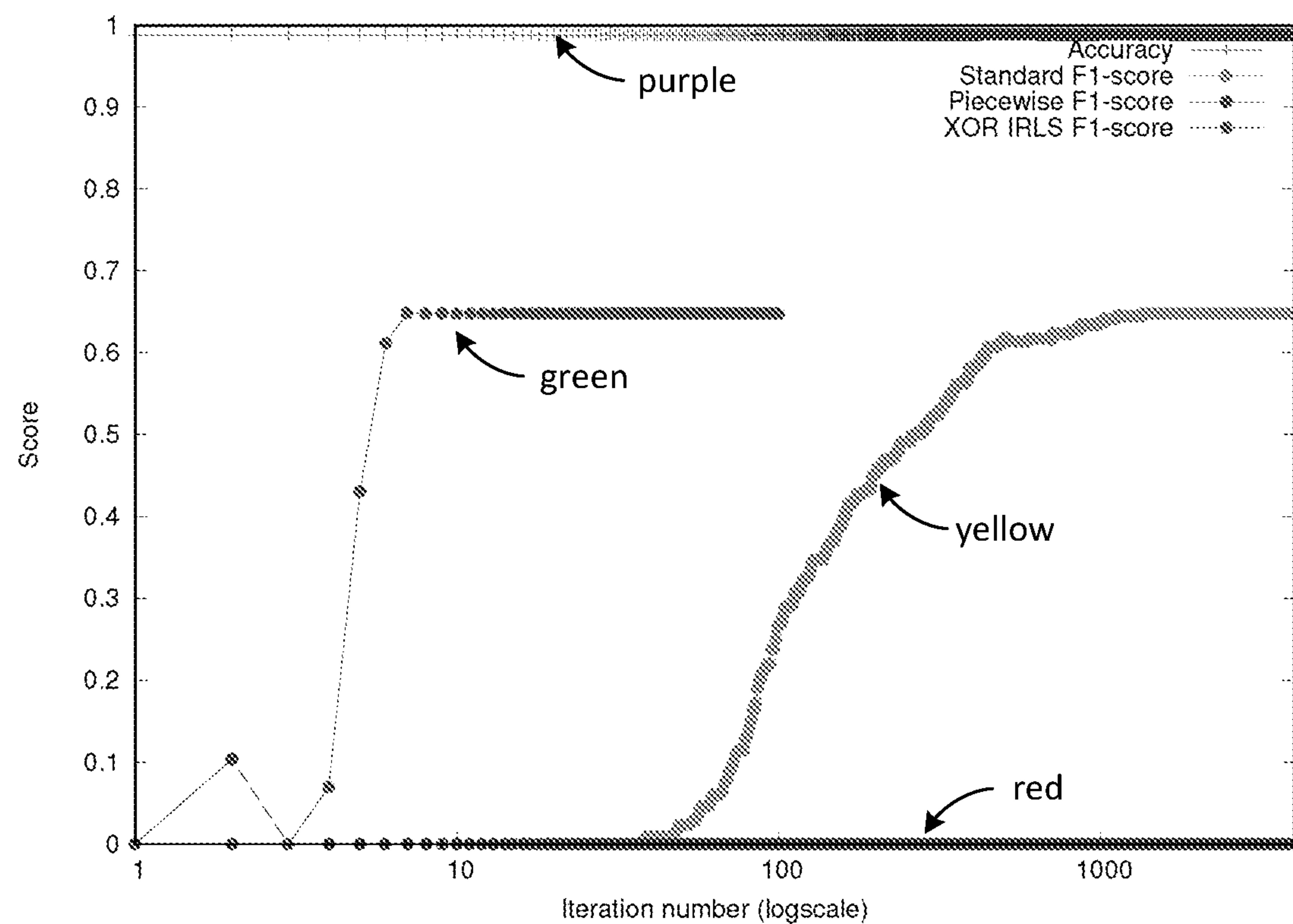


FIG. 8

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)

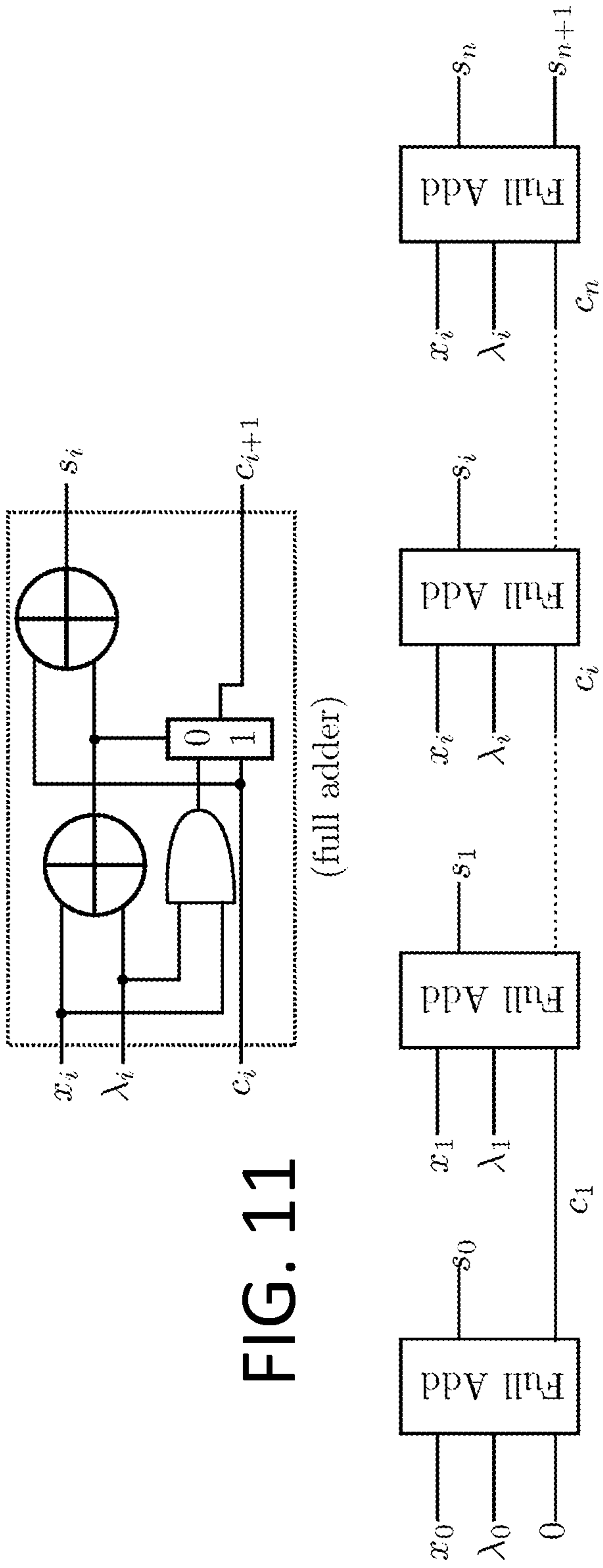
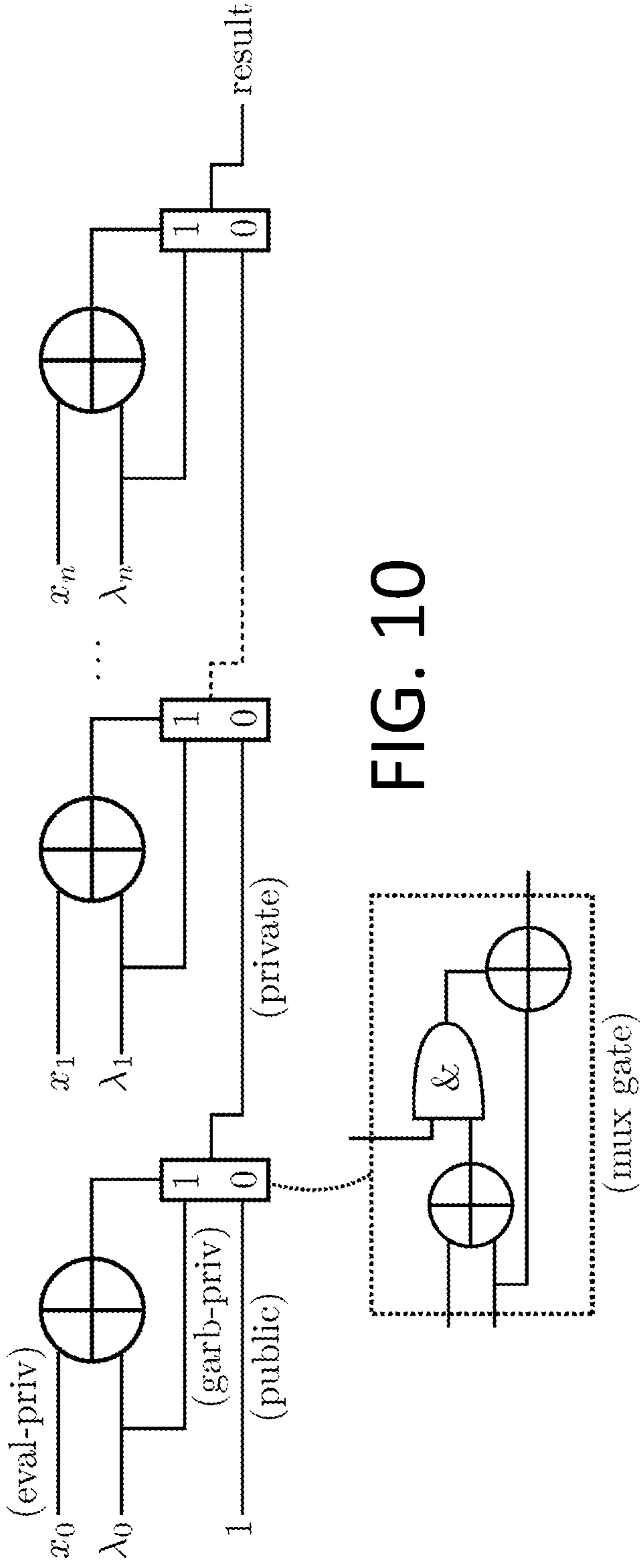


FIG. 12

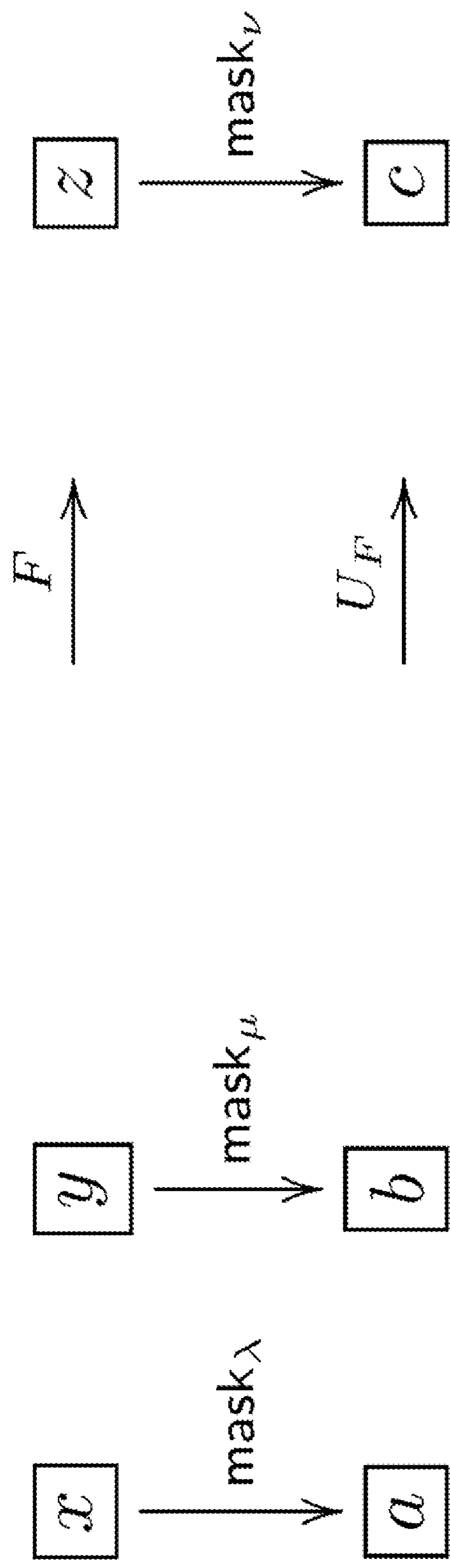


FIG. 13

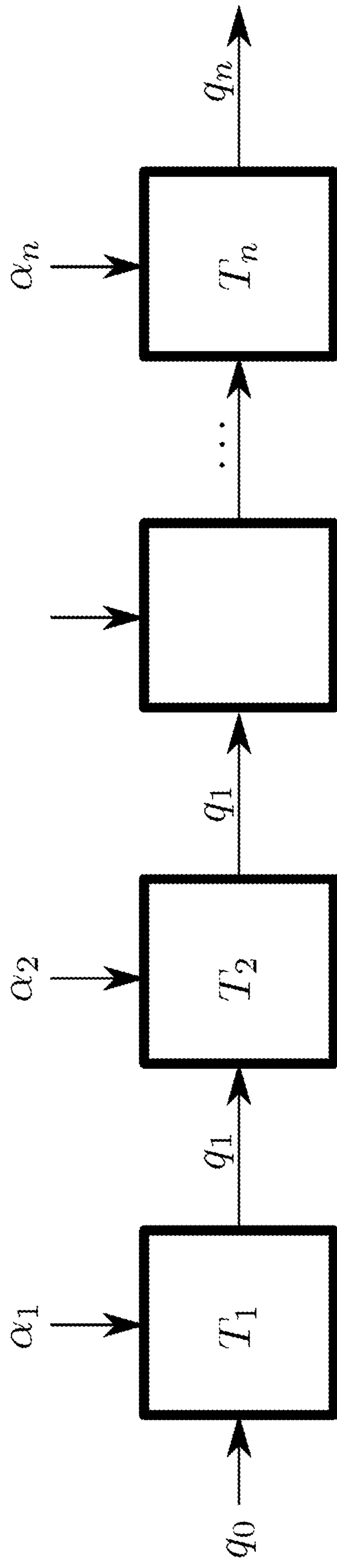


FIG. 14

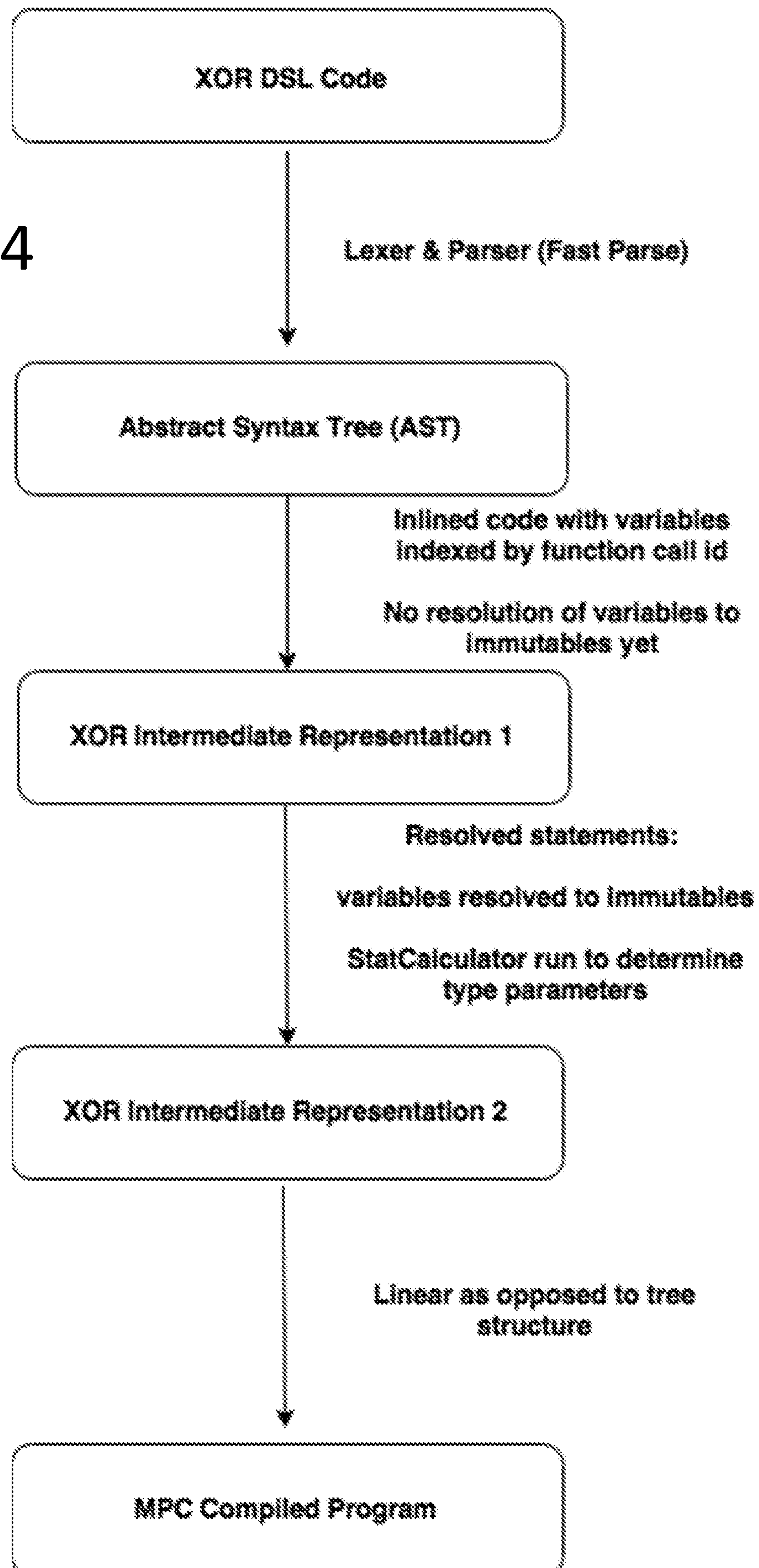


FIG. 15

1500

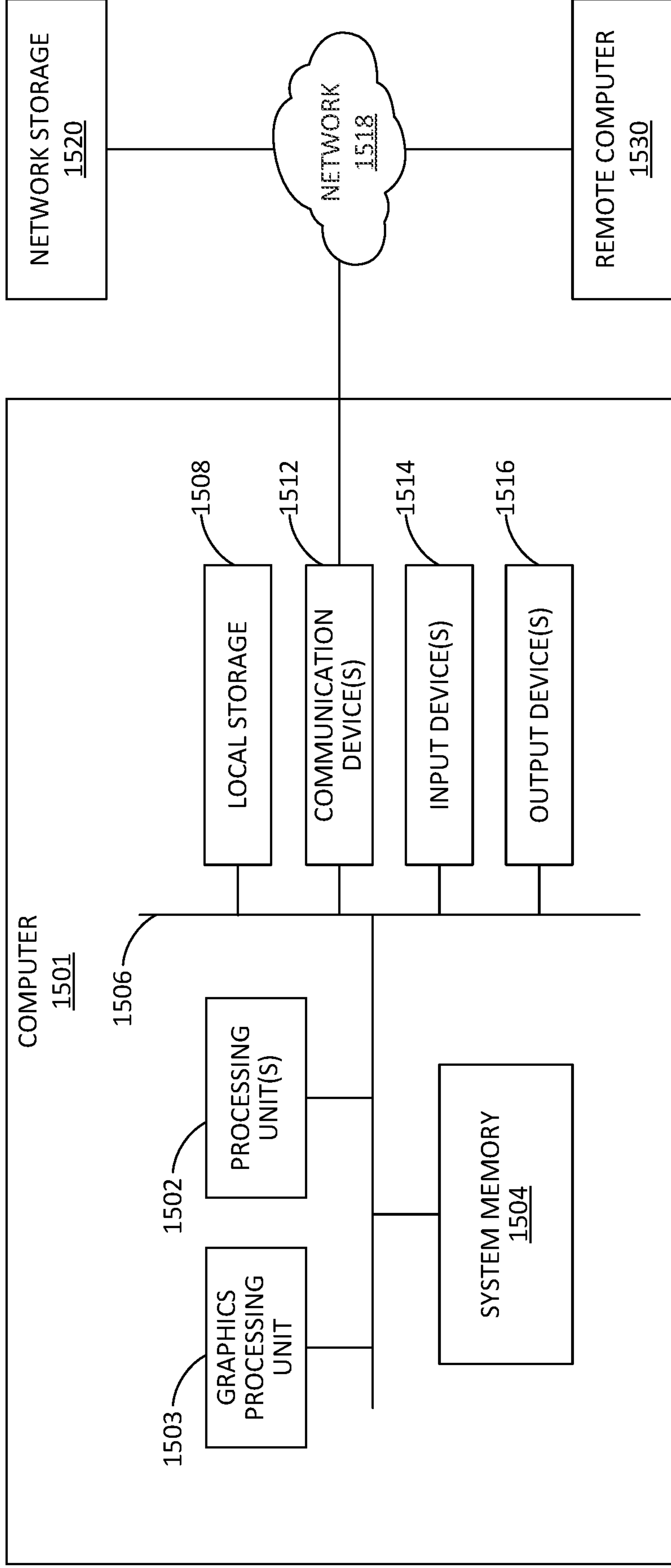


FIG. 16

A method for performing secure multi-party computations produces a result while preserving privacy of input data contributed by individual parties as follows

a dealer computing system creates a plurality of sets of related numerical masking data components, wherein for each set of related numerical masking data components, each component of the set is one of: a scalar, a vector and a matrix

the dealer computing system secret shares, among a plurality of party computing systems, each component of each set of the plurality of sets of related numerical masking data components

for each party computing system of the plurality of party computing systems, the party computing system:

receives a respective secret share of each component of each set of the plurality of sets of numerical masking data components from the trusted dealer

executes a set of program instructions that cause the party computing system to perform, in conjunction and communication with others of the party computing systems, one or more multi-party computations to create one or more instances of computed secret shared data, wherein for each instance, the party computing system computes a secret share of the instance based on at least one secret share of a set of input data or at least one secret share of another instance of computed secret shared data, wherein received secret shares of numerical masking data components are used to mask data communicated during the computations, and wherein the computations include at least one of (a) and (b) as follows:

(a) a Fourier series approximation or an approximation using trigonometric polynomials, of a continuous function;

(b) a secret share reduction that transforms an instance of computed secret shared data stored in floating-point representation into an equivalent, equivalently precise, and equivalently secure instance of computed secret shared data having a reduced memory storage requirement

transmits a secret share of an instance of computed secret shared data to one or more others of the plurality of party computing systems

for at least one party computing system of the plurality of party computing systems, the party computing system:

receives one or more secret shares of an instance of computed secret shared data from one or more others of the plurality of party computing systems

combines the received secret shares of the instance of computed secret shared data to produce the result