

ISO/IEC 4922-1:2023-07 (E)

Information security - Secure multiparty computation - Part 1: General

Contents		Page
Foreword		iv
Introduction		v
1	Scope	1
2	Normative references	1
3	Terms and definitions	1
4	General model and parameters	2
4.1	Generic model	2
4.2	Parameters of secure multiparty computation	4
4.2.1	Overview	4
4.2.2	Input space	4
4.2.3	Encoded space	4
4.2.4	Output space	4
4.2.5	The number of computing parties	4
4.2.6	Role restriction	4
4.2.7	Communication model	4
4.2.8	Summary of parameters	5
5	Properties and analysis of secure multiparty computation	5
5.1	Fundamental requirements	5
5.1.1	Overview	5
5.1.2	Correctness	5
5.1.3	Input privacy	5
5.2	Adversary model	5
5.2.1	Overview	5
5.2.2	Adversary behaviour	6
5.2.3	Number of corruptions	6
5.2.4	Computational power	6
5.2.5	Composition and parallel execution	7
5.2.6	Network access	7
5.3	Optional properties	7
5.3.1	Overview	7
5.3.2	Correctness against active adversary	7
5.3.3	Input privacy against active adversary	7
5.3.4	Fairness	8
5.3.5	Guaranteed output delivery	8
5.4	Performance properties for the comparison of schemes	8
5.4.1	Overview	8
5.4.2	Communication efficiency	8
5.4.3	Computational efficiency	8
Annex A (informative)	Possible use cases for secure multiparty computation	9
Bibliography		10