

# ISO/IEC 19592-1:2016-11 (E)

## Information technology - Security techniques - Secret sharing - Part 1: General

---

<b>Contents</b>		<b>Page</b>
Foreword .....		iv
Introduction .....		v
1	Scope .....	1
2	Normative references .....	1
3	Terms and definitions .....	1
4	General model of secret sharing .....	2
4.1	Parties involved .....	2
4.2	Parameters .....	3
4.2.1	Overview .....	3
4.2.2	Message space .....	3
4.2.3	Share space .....	3
4.2.4	Number of shares .....	3
4.2.5	Access structure .....	3
4.3	Message sharing process .....	4
4.4	Message reconstruction process .....	4
5	Properties of secret sharing schemes .....	5
5.1	Fundamental requirements .....	5
5.1.1	Overview .....	5
5.1.2	Message confidentiality .....	6
5.1.3	Message recoverability .....	6
5.2	Optional requirements .....	6
5.2.1	Overview .....	6
5.2.2	Homomorphicity .....	6
5.2.3	Verifiability .....	6
5.3	Other properties .....	7
5.3.1	Overview .....	7
5.3.2	Confidentiality guarantees .....	7
5.3.3	Complexity .....	7
5.3.4	Information rate .....	7