

ISO/IEC 4922-2:2024-03 (E)

Information security - Secure multiparty computation - Part 2: Mechanisms based on secret sharing

Contents

Page

- Foreword..... v
- Introduction..... vi
- 1 Scope..... 1
- 2 Normative references..... 1
- 3 Terms and definitions..... 1
- 4 Symbols and abbreviated terms..... 3
- 5 Secure multiparty computation based on secret sharing..... 3
 - 5.1 General..... 3
 - 5.2 Secret sharing..... 4
 - 5.3 Secure multiparty computation based on secret sharing..... 4
- 6 Addition, subtraction, and multiplication by a constant..... 5
 - 6.1 General..... 5
 - 6.2 Addition..... 5
 - 6.2.1 Addition for the Shamir secret sharing scheme..... 5
 - 6.2.2 Addition of a constant for the Shamir secret sharing scheme..... 6
 - 6.2.3 Addition for the replicated additive secret sharing scheme..... 6
 - 6.2.4 Addition of a constant for the replicated additive secret sharing scheme..... 6
 - 6.3 Subtraction..... 7
 - 6.3.1 Subtraction for the Shamir secret sharing scheme..... 7
 - 6.3.2 Subtraction of a constant for the Shamir secret sharing scheme..... 7
 - 6.3.3 Subtraction for the replicated additive secret sharing scheme..... 8
 - 6.3.4 Subtraction of a constant for the replicated additive secret sharing scheme..... 8
 - 6.4 Multiplication by a constant..... 9
 - 6.4.1 Multiplication by a constant for the Shamir secret sharing scheme..... 9
 - 6.4.2 Multiplication by a constant for the replicated additive secret sharing scheme..... 9
- 7 Shared random number generation..... 10
 - 7.1 General..... 10
 - 7.2 Information-theoretically secure shared random number generation..... 10
 - 7.2.1 General-purpose shared random number generation scheme..... 10
 - 7.2.2 Shared random number generation for the replicated additive secret sharing scheme..... 11
 - 7.2.3 Shared random number generation for the Shamir secret sharing scheme..... 11
 - 7.3 Computationally secure shared random number generation..... 12
 - 7.3.1 General..... 12
 - 7.3.2 Seed sharing phase..... 13
 - 7.3.3 Shared random number generation phase for the replicated additive secret sharing scheme..... 13
 - 7.3.4 Shared random number generation phase for the Shamir secret sharing scheme..... 14
- 8 Multiplication..... 15
 - 8.1 General..... 15
 - 8.2 GRR-multiplication for the Shamir secret sharing scheme..... 15
 - 8.2.1 General..... 15
 - 8.2.2 Parameters..... 15
 - 8.2.3 Multiplication protocol..... 15
 - 8.2.4 Dot product protocol..... 16
 - 8.2.5 Properties..... 16

8.3	DN-multiplication for the Shamir secret sharing scheme.....	16
8.3.1	General.....	16
8.3.2	Parameters.....	17
8.3.3	Multiplication protocol.....	17
8.3.4	Dot product protocol.....	17
8.3.5	Properties.....	18
8.4	CHIKP-multiplication for the replicated additive secret sharing scheme.....	18
8.4.1	General.....	18
8.4.2	Parameters.....	18
8.4.3	Multiplication protocol.....	18
8.4.4	Properties.....	18
8.5	Beaver-multiplication.....	19
8.5.1	General.....	19
8.5.2	Parameters.....	19
8.5.3	Multiplication protocol.....	19
8.5.4	Properties.....	19
9	Secure function evaluation.....	20
Annex A	(normative) Object identifiers.....	21
Annex B	(informative) Numerical examples.....	23
Annex C	(informative) Security considerations.....	32
Bibliography	33