ISO/IEC 18033-6:2019 (E)

IT Security techniques — Encryption algorithms — Part 6: Homomorphic encryption

Contents

Foreword

Introduction

1 Scope

2 Normative references

3 Terms and definitions

4 Symbols and abbreviations

5 General model for homomorphic encryption

5.1 Entities
5.2 Key roles
5.3 Algorithms
5.4 Functional requirements

6 Homomorphic encryption mechanisms

6.1 General
6.2 Exponential ElGamal encryption
6.2.1 General
6.2.2 Key generation algorithm
6.2.3 Encryption
6.2.4 Decryption
6.3 Paillier encryption
6.3.1 General
6.3.2 Key generation algorithm
6.3.3 Encryption
6.3.4 Decryption

Annex A (normative) Object identifiers

Annex B (informative) Numerical examples

B.1 Exponential ElGamal encryption
B.1.1 General
B.1.2 1 024-bit finite field, 160-bit security parameter, 2-party
B.1.2.1 Key generation
B.1.2.2 Encryption and decryption
B.1.2.3 Homomorphic map
B.2 Paillier encryption
B.2.1 General
B.2.2 1 024-bit finite field, 160-bit security parameter
B.2.2.1 Key generation
B.2.2.2 Encryption and decryption
B.2.2.3 Homomorphic map

Page count: 17