ISO/IEC 14888-4:2024-06 (E)

Information security - Digital signatures with appendix - Part 4: Stateful hash-based mechanisms

Contents

Page

Foreword ..... **v**

Introduction ..... **vi**

1 Scope **1**

2 Normative references **1**

3 Terms and definitions **1**

4 Symbols and abbreviated terms **2**
4.1 Symbols 2
4.2 Abbreviated terms 3

5 XMSS and XMSS-MT **3**
5.1 General 3
5.2 Common building blocks 3
5.2.1 General 3
5.2.2 Address format 3
5.2.3 Required cryptographic functions 4
5.2.4 Auxiliary functions 6
5.2.5 WOTS+ One-Time Signature Auxiliary Scheme 7
5.3 XMSS Algorithms 10
5.3.1 General 10
5.3.2 Auxiliary functions 10
5.3.3 XMSS Key Generation 12
5.3.4 XMSS Signing 14
5.3.5 XMSS Authentication Path Computation 15
5.3.6 XMSS Verification 15
5.4 XMSS-MT Algorithms 17
5.4.1 General 17
5.4.2 XMSS-MT key Generation 17
5.4.3 XMSS-MT signing 18
5.4.4 XMSS-MT Verification 19
5.5 Suggested parameters 20

6 LMS and HSS schemes **21**
6.1 Byte ordering convention 21
6.2 Converting to base 2^W 21
6.3 Checksum Calculation 21
6.4 Type code 22
6.5 LM-OTS 22
6.5.1 General 22
6.5.2 Key generation 22
6.5.3 Signing 23
6.5.4 Verification 24
6.5.5 Suggested Parameters 24
6.6 LMS 25
6.6.1 General 25
6.6.2 Key generation 25
6.6.3 Signing 26
6.6.4 Verification 26
6.6.5 Suggested Parameters 27

6.7 HSS 27
6.7.1 General 27
6.7.2 Key generation 28
6.7.3 Signing 29
6.7.4 Verification 29
6.7.5 Suggested Parameters 30
7 State management **30**
Annex A (normative) **Object identifiers and ASN.1 module** **31**
Annex B (informative) **Relation to other standards** **33**
Annex C (informative) **Numerical examples** **34**
Bibliography **56**