ISO/IEC 9797-2:2011-05 (E)

Information technology - Security techniques - Message Authentication Codes (MACs) - Part 2: Mechanisms using a dedicated hash-function

Contents

Page

Foreword iv

Introduction v

1 Scope 1

2 Normative references 1

3 Terms and definitions 2

4 Symbols and notation 4

5 Requirements 5

6 MAC Algorithm 1 6
6.1 Description of MAC Algorithm 1 7
6.1.1 Step 1 (key expansion) 7
6.1.2 Step 2 (modification of the constants and the IV) 7
6.1.3 Step 3 (hashing operation) 7
6.1.4 Step 4 (output transformation) 8
6.1.5 Step 5 (truncation) 8
6.2 Efficiency 8
6.3 Computation of the constants 8
6.3.1 Dedicated Hash-Function 1 (RIPEMD-160) 9
6.3.2 Dedicated Hash-Function 2 (RIPEMD-128) 9
6.3.3 Dedicated Hash-Function 3 (SHA-1) 10
6.3.4 Dedicated Hash-Function 4 (SHA-256) 10
6.3.5 Dedicated Hash-Function 5 (SHA-512) 10
6.3.6 Dedicated Hash-Function 6 (SHA-384) 11
6.3.7 Dedicated Hash-Function 8 (SHA-224) 11

7 MAC Algorithm 2 12
7.1 Description of MAC Algorithm 2 12
7.1.1 Step 1 (key expansion) 12
7.1.2 Step 2 (hashing operation) 12
7.1.3 Step 3 (output transformation) 12
7.1.4 Step 4 (truncation) 13
7.2 Efficiency 13

8 MAC Algorithm 3 13
8.1 Description of MAC Algorithm 3 13
8.1.1 Step 1 (key expansion) 13
8.1.2 Step 2 (modification of the constants and the IV) 14
8.1.3 Step 3 (padding) 14
8.1.4 Step 4 (application of the round-function) 14
8.1.5 Step 5 (truncation) 15
8.2 Efficiency 15

Annex A (normative) ASN.1 Module 16

Annex B (informative) Examples 17

Annex C (informative) A security analysis of the MAC algorithms 37

Bibliography 39