ISO/IEC 9797-2:2002-06 (E)

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

Contents

Page

1 Scope 1 2 Normative references 1 3 Terms and definitions 1 4 Symbols and notation 2 5 Requirements 3 6 MAC Algorithm 1 3 6.1 Description of MAC Algorithm 1 4

6.1.1 Step 1 (key expansion) 4
6.1.2 Step 2 (modification of the constants and the IV) 4
6.1.3 Step 3 (hashing operation) 4
6.1.4 Step 4 (output transformation) 4
6.1.5 Step 5 (truncation) 4
6.2 Efficiency 4
6.3 Computation of the constants 4
6.3.1 Dedicated Hash-Function 1 5
6.3.2 Dedicated Hash-Function 2 5
6.3.3 Dedicated Hash-Function 3 5

7 MAC Algorithm 2 5 7.1 Description of MAC Algorithm 2 6
7.1.1 Step 1 (key expansion) 6
7.1.2 Step 2 (hashing operation) 6
7.1.3 Step 3 (output transformation) 6
7.1.4 Step 4 (truncation) 6
7.2 Efficiency 6

8 MAC Algorithm 3 6 8.1 Description of MAC Algorithm 3 6
8.1.1 Step 1 (key expansion) 6
8.1.2 Step 2 (modification of the constants and the IV) 7
8.1.3 Step 3 (padding) 7
8.1.4 Step 4 (application of the round-function) 7
8.1.5 Step 5 (truncation) 7
8.2 Efficiency 7