ISO/IEC 29192-6:2019 (E)

Information technology — Lightweight cryptography — Part 6: Message authentication codes (MACs)

Contents

Foreword

Introduction

1 Scope

2 Normative references

3 Terms and definitions

4 Symbols and abbreviated terms

5 Lightweight MACs based on block ciphers

- 5.1 General
- 5.2 LightMAC
- 5.2.1 General
- 5.2.2 Step 1 (padding)
- 5.2.3 Step 2 (application of the block cipher)
- 5.2.4 Step 3 (truncation)

6 Lightweight MACs based on hash-functions

- 6.1 General
- 6.2 Tsudik's keymode
- 6.2.1 Requirements
- 6.2.2 MAC calculation

7 Lightweight dedicated MACs

- 7.1 General
- 7.2 Chaskey-12
- 7.2.1 General
- 7.2.2 Step 1 (subkey derivation)
- 7.2.3 Step 2 (padding)
- 7.2.4 Step 3 (application of the permutation)
- 7.2.5 Step 4 (truncation)

Annex A (normative) Object identifiers

Annex B (informative) Numerical examples

- B.1 General
- B.2 Numerical examples of LightMAC
- B.3 Numerical example of Tsudik's keymode
- B.4 Numerical examples of Chaskey-12

Annex C (informative) Security information and feature tables

- C.1 General
- C.2 Information on LightMAC
- C.2.1 Lightweight properties of LightMAC
- C.2.2 Parameter s
- C.3 Information on the underlying hash-functions to be used in Tsudik's mode
- C.4 Information on the usage of Chaskey-12

Annex D (informative) Specification of I2BS

- D.1 General
- D.2 I2BS