INTERNATIONAL STANDARD

ISO/IEC 10118-4

First edition
1998-12-15

AMENDMENT 1
2014-11-15

Information technology — Security techniques — Hash-functions —

Part 4: Hash-functions using modular arithmetic

AMENDMENT 1: Object identifiers

Technologies de l'information — Techniques de sécurité — Fonctions de brouillage —

Partie 4: Fonctions de hachage utilisant l'arithmétique modulaire

AMENDEMENT 1: Identificateurs d'objet

Reference number
ISO/IEC 10118-4:1998/Amd.1:2014(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 10118-4 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Security technology*.

Amendment 1 to ISO/IEC 10118-4:1998 was written to serve two purposes.

First, a new normative Annex C is produced for the object identifiers assigned to the hash-functions included in ISO/IEC 10118-4:1998.

Second, the present Annex C for Bibliography is moved to the end of the text, after the new Annex C according to ISO/IEC Directives, Part 2.

Information technology — Security techniques — Hash-functions —

Part 4:
Hash-functions using modular arithmetic

AMENDMENT 1: Object identifiers

Page 23

Replace the present Annex C with the following Annex C, and add the following Bibliography.

Annex C

(normative)

Object identifiers

This annex lists object identifiers assigned to the hash-functions using modular arithmetic specified in this part of ISO/IEC 10118.

```
--
-- ISO/IEC 10118-4 ASN.1 Module
--
HashFunctionsUsingModularArithmetic {
       iso(1) standard(0) hash-functions(10118) part4(4)
              asn1-module(1) hash-functions-using-modular-arithmetic(0)}
       DEFINITIONS EXPLICIT TAGS ::= BEGIN
-- EXPORTS All; --
-- IMPORTS None; --
OID ::= OBJECT IDENTIFIER -- Alias
-- Synonyms --
id-hfma OID ::= {
       iso(1) standard(0) hash-functions(10118) part4(4) algorithms(0) }
-- Assignments --
id-hfma-mash1 OID ::= { id-hfma mash1(65) }
id-hfma-mash2 OID ::= { id-hfma mash2(66) }
-- NOTE - Assign any new OIDs above 66 to additional algorithms --
}
END -- HashFunctionsUsingModularArithmetic --
```

Bibliography

[1] BONEH D., & FRANKLIN M. *Efficient Generation of Shared RSA Keys*. Advances in Cryptology - CRYPTO '97 (BURTON S., & KALISKI Jr. ed.) Lecture Notes in Computer Science, **Vol. 1294**, Springer-Verlag, 1997, pp. 425-439.

[2] COCKS C. *Split knowledge generation of RSA parameters*. Cryptography and Coding. (DARELL M. ed.). Lecture Notes in Computer Science, **Vol. 1355**, Springer-Verlag, 1997, pp. 89–95.

[3] FRANKEL Y., MACKENZIE P.D., YUNG M. *Robust efficient distributed RSA-key generation*. Proceedings of the 30th Annual ACM Symposium on the Theory of Computing (STOC '98), ACM, 1998, pp. 663-672.