INTERNATIONAL STANDARD ISO/IEC 10118-4:1998
TECHNICAL CORRIGENDUM 1

Published 2014-07-15

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION • МЕЖДУНАРОДНАЯ ОРГАНИЗАЦИЯ ПО СТАНДАРТИЗАЦИИ • ORGANISATION INTERNATIONALE DE NORMALISATION
INTERNATIONAL ELECTROTECHNICAL COMMISSION • МЕЖДУНАРОДНАЯ ЭЛЕКТРОТЕХНИЧЕСКАЯ КОМИССИЯ • COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

Information technology — Security techniques — Hash-functions —

Part 4:
Hash-functions using modular arithmetic

TECHNICAL CORRIGENDUM 1

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

Partie 4: Fonctions de hachage utilisant l'arithmétique modulaire

RECTIFICATIF TECHNIQUE 1

Technical Corrigendum 1 to ISO/IEC 10118-4:1998 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*

Page 4, Subclause 5.1

Add the following text immediately after 5.1.5:

5.1.6 The modulus N of the MASH-1 round-function shall not satisfy either of the following two conditions:

The left-most bit of N is equal to 1, and the next L_ϕ bits are equal to 0.

$L_N = L_\phi + 1$, $N \neq 31 \pmod{32}$, the 4 left-most bits of N are equal to 1, the bits of N at positions $8t_1 + t_2$, $t_1 = 0, 1, \ldots, L_\phi / 8$, $t_2 \in \{5, 6, 7\}$ are equal to 1, and every 5-tuple $8t_1, 8t_1 + 1, \ldots, 8t_1 + 4$, $t_1 = 1, 2, \ldots, L_\phi / 8$ contains at least one bit equal to 1.

ICS 35.040 **Ref. No. ISO/IEC 10118-4:1998/Cor.1:2014(E)**

Published in Switzerland