

PN-ISO/IEC 10118-4:2001/AC1

Wprowadza
ISO/IEC 10118-4:1998/AC1:2014, IDT

Technika informatyczna

Techniki zabezpieczeń

Funkcje skrótu

**Część 4: Funkcje skrótu wykorzystujące
arytmetykę modularną**

Poprawka do Normy Międzynarodowej ISO/IEC 10118-4:1998/AC1:2014 *Information technology — Security techniques — Hash-functions — Part 4: Hash-functions using modular arithmetic* ma status Poprawki do Polskiej Normy

Przedmowa krajowa

Niniejsza poprawka została zatwierdzona przez Prezesa PKN dnia 28 maja 2019 r.

Komitetem krajowym odpowiedzialnym za poprawkę jest KT nr 182 ds. Ochrony Informacji w Systemach Teleinformatycznych.

Istnieje możliwość przetłumaczenia poprawki na język polski na wniosek zainteresowanych środowisk. Decyzję podejmuje właściwy Komitet Techniczny.

W sprawach merytorycznych dotyczących treści normy można zwracać się do właściwego Komitetu Technicznego lub właściwej Rady Sektorowej PKN, kontakt: www.pkn.pl

Nota uznaniowa

Poprawka do Normy Międzynarodowej ISO/IEC 10118-4:1998/AC1:2014 została uznana przez PKN za Poprawkę do Polskiej Normy PN-ISO/IEC 10118-4:2001/AC1:2019-05.



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 $8t_1 + t_2$, $t_1 = 0, 1, \dots, L_\phi / 8$, $t_2 \in \{5, 6, 7\}$ are equal to 1, and every 5-tuple $8t_1, 8t_1 + 1, \dots, 8t_1 + 4$, $t_1 = 1, 2, \dots, L_\phi / 8$ contains at least one bit equal to 1.

Page 23, Bibliography

Add the following to the end of the bibliography:

- [4] Antipkin V.G. *Smashing MASH-1*, Mathematical Aspects of Cryptography, 2014, Volume 5, Issue 2, pages 21-28.