POLSKI KOMITET NORMALIZACYJNY

POPRAWKA do POLSKIEJ NORMY

ICS 35.030

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

© Copyright by PKN, Warszawa 2019 **nr ref. PN-ISO/IEC 10118-4:2001/AC1:2019-05**

Wszelkie prawa autorskie zastrzeżone. Żadna część niniejszej publikacji nie może być zwielokrotniana jakąkolwiek techniką bez pisemnej zgody Prezesa Polskiego Komitetu Normalizacyjnego

Przedmowa krajowa

Niniejsza poprawka jest tłumaczeniem angielskiej wersji Poprawki do Normy Międzynarodowej ISO/IEC 10118-4:1998/AC1:2014.

Została zatwierdzona przez Prezesa PKN dnia 28 maja 2019 r.

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

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

Treść poprawki

Strona 8, Podrozdział 5.1

Dodano następujacy tekst bezpośrednio po 5.1.5:

5.1.6 Moduł *N* funkcji rundy MASH-1 nie powinien spełniać żadnego z następujących dwóch warunków:

Lewy skrajny bit *N* jest równy 1, a następne bity L_ϕ są równe 0.

$L_N = L_\phi + 1$, $N \neq 31 (\mathrm{mod}\ 32)$, 4 lewe skrajne bity *N* są równe 1, bity *N* w pozycjach $8t_1 + t_2$, $t_1 = 0,1,..., L_\phi / 8$, $t_2 \in \{5, 6, 7\}$ są równe 1, a każda 5-krotna $8t_1$, $8t_1 + 1,..., 8t_1 + 4$, $t_1 = 1,2,..., L_\phi / 8$ zawiera co najmniej jeden bit równy 1.

Strona 25, Bibliografia

Dodano następującą pozycję na końcu bibliografii:

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