



INTERNATIONAL STANDARD ISO/IEC 15946-5:2009
TECHNICAL CORRIGENDUM 1

Published 2012-12-01

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 — Cryptographic techniques based on elliptic curves —

Part 5: Elliptic curve generation

TECHNICAL CORRIGENDUM 1

Technologies de l'information — Techniques de sécurité — Techniques cryptographiques fondées sur les courbes elliptiques —

Partie 5: Génération de courbes elliptiques

RECTIFICATIF TECHNIQUE 1

Technical Corrigendum 1 to ISO/IEC 15946-5:2009 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

Page v, Introduction, paragraph 3

Replace:

"defined in ISO/IEC 9796-3, ISO/IEC 11770-3, ISO/IEC 14888-3, and ISO/IEC 18033-2."

with:

"defined in ISO/IEC 9796-3, ISO/IEC 11770-3, ISO/IEC 14888-3, ISO/IEC 18033-2 and ISO/IEC 29192-4."

ICS 35.040

Ref. No. ISO/IEC 15946-5:2009/Cor.1:2012(E)

© ISO/IEC 2012 – All rights reserved

Published in Switzerland

AVA Documents
Document Sharing Hub

Page 1, Scope, paragraph 2

Replace:

"defined in ISO/IEC 9796-3, ISO/IEC 11770-3, ISO/IEC 14888-3 and ISO/IEC 18033-2."

with:

"defined in ISO/IEC 9796-3, ISO/IEC 11770-3, ISO/IEC 14888-3, ISO/IEC 18033-2 and ISO/IEC 29192-4."

Page 6, 6.1.4 d)

Delete "1) Compute $Z = Z + i \bmod 2^L$."

Replace:

"2) Convert $Z \bmod(2^L)$ to a bit string $X_i = \text{I2BSP}(Z)$."

with:

"1) Convert $Z+i \bmod 2^L$ to a bit string $X_i = \text{I2BSP}(Z)$."

Replace:

"3) Compute $W_i = H(X_i)$."

with:

"2) Compute $W_i = H(X_i)$."

Page 19, Annex B.2.3, line 2

Replace "A value B is given as the smallest integer such that n divides $p^B - 1$."

with:

"A value B , used for the MOV-condition, is given as the smallest integer such that n divides $p^B - 1$."