



INTERNATIONAL STANDARD ISO/IEC 15946-1:2008
TECHNICAL CORRIGENDUM 2

Published 2014-04-01

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 1: General

TECHNICAL CORRIGENDUM 2

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

Partie 1: Généralités

RECTIFICATIF TECHNIQUE 2

Technical Corrigendum 2 to ISO/IEC 15946-1:2008 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*. Corrigendum 2 cancels and replaces ISO/IEC 15946-1:2008/Cor.1:2009.

Page iii, Contents

Add the following entry above the entry for Bibliography:

Annex D (informative) Summary of coordinates 28

ICS 35.040

Ref. No. ISO/IEC 15946-1:2008/Cor.2:2014(E)

© ISO/IEC 2014 – All rights reserved

Published in Switzerland

AVA Documents
Document Sharing Hub

Page iv, Foreword

Replace:

— *Part 3: Key establishment*

with:

— *Part 5: Elliptic curve generation*

and delete the following:

"Elliptic curve generation will form the subject of a future Part 5."

Page 1, 2.2

Convert the existing NOTE to NOTE 1 and add the following new NOTE:

NOTE 2 A definition of a cubic curve is given in bibliography item [16].

Page 25, C.4.2 Algorithm to compute the Weil pairing

Replace:

b) Compute $e_n(G_1, G_2) = (d_n(G_2, G_1 + R) d_n(G_1, -R)) / (d_n(G_2, R) d_n(G_1, G_2 - R))$.

with:

b) Compute $e_n(G_1, G_2) = (d_n(G_2, R) d_n(G_1, G_2 - R)) / (d_n(G_2, G_1 + R) d_n(G_1, -R))$.

Page 30, Bibliography

Delete item [3].

Page 30, Bibliography

Replace:

[4] ISO/IEC 15946-5:—¹⁾, *Information technology — Security techniques — Cryptographic techniques based on elliptic curves — Part 5: Elliptic curve generation*

with:

[4] ISO/IEC 15946-5:2009, *Information technology — Security techniques — Cryptographic techniques based on elliptic curves — Part 5: Elliptic curve generation*

Page 30, Bibliography

Delete the following footnote:

1) To be published.