INTERNATIONAL STANDARD ISO/IEC 18033-3:2005
TECHNICAL CORRIGENDUM 2

Published 2007-09-01

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 — Encryption algorithms —

Part 3: Block ciphers

TECHNICAL CORRIGENDUM 2

Technologies de l'information — Techniques de sécurité — Algorithmes de chiffrement —

Partie 3: Chiffrements par blocs

RECTIFICATIF TECHNIQUE 2

Technical Corrigendum 1 to ISO/IEC 18033-3:2005 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

ICS 35.040 **Ref. No. ISO/IEC 18033-3:2005/Cor.2:2007(E)**

© ISO/IEC 2007 – All rights reserved

Published in Switzerland

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

Not for Resale

Replace Figures 22 and 24 with the following figures.

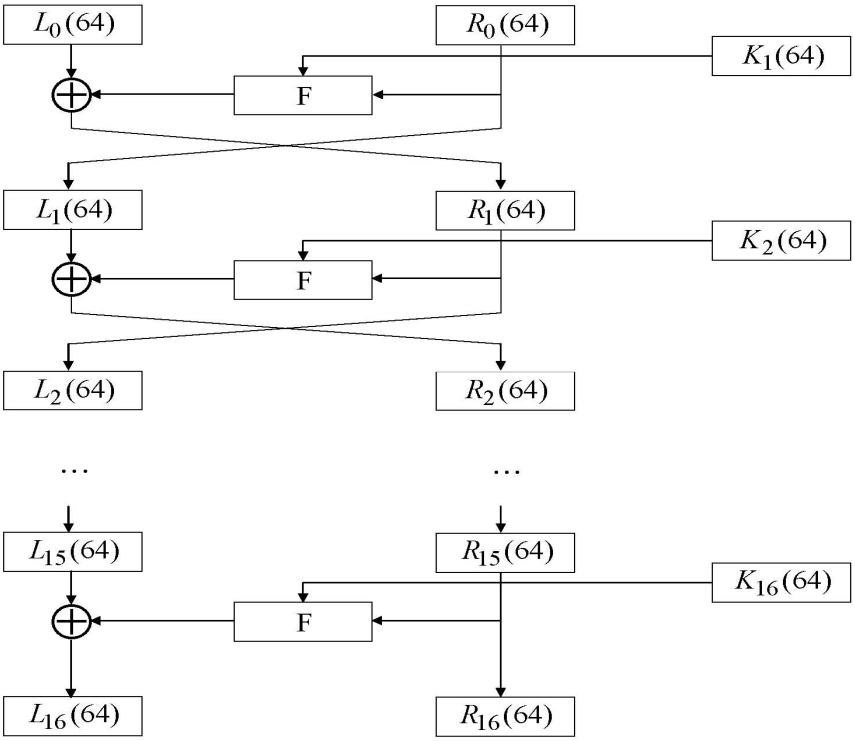

Figure 22 — Structure of SEED

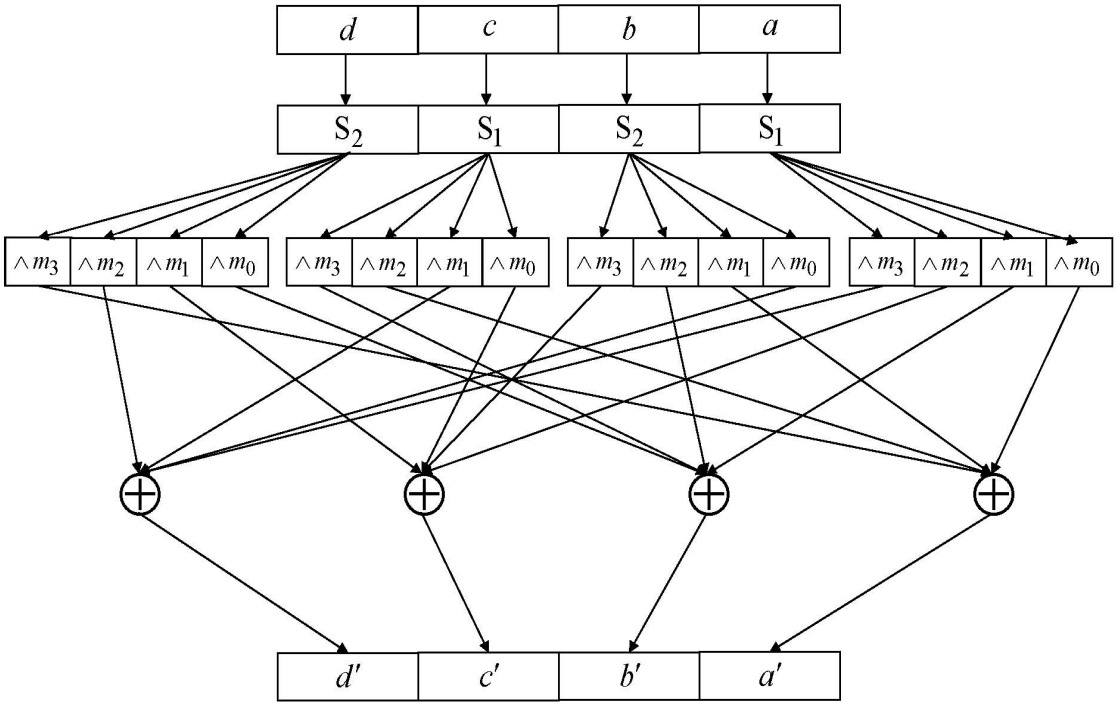

Figure 24 — The Function G

© ISO/IEC 2007 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale