



BSI Standards Publication

Information security — Encryption algorithms

Part 7: Tweakable block ciphers

National foreword

This British Standard is the UK implementation of ISO/IEC 18033-7:2022.

The UK participation in its preparation was entrusted to Technical Committee IST/33/2, Cryptography and Security Mechanisms.

A list of organizations represented on this committee can be obtained on request to its committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

© The British Standards Institution 2022
Published by BSI Standards Limited 2022

ISBN 978 0 539 14351 5

ICS 35.030

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 June 2022.

Amendments/corrigenda issued since publication

Date	Text affected
------	---------------

Information security — Encryption algorithms —

Part 7: Tweakable block ciphers

*Sécurité de l'information — Algorithmes de chiffrement —
Partie 7: Chiffrements par blocs paramétrables*





COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2022

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword	iv
Introduction	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Symbols	2
5 Requirements on the usage of tweakable block ciphers	3
6 Deoxys-TBC	3
6.1 Deoxys-TBC versions.....	3
6.2 Deoxys-TBC encryption.....	4
6.3 Deoxys-TBC decryption.....	5
6.4 Deoxys-TBC tweakkey schedule.....	6
7 Skinny	7
7.1 Skinny versions.....	7
7.2 Skinny encryption.....	8
7.3 Skinny decryption.....	10
7.4 Skinny tweakkey schedule.....	11
Annex A (informative) Numerical examples	14
Annex B (normative) Object identifiers	16
Bibliography	18

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see patents.iec.ch).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

A list of all parts in the ISO/IEC 18033 series can be found on the ISO and IEC websites.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

Introduction

This document specifies tweakable block ciphers. A tweakable block cipher is a family of permutations parametrized by a secret key value and a public tweak value.

Information security — Encryption algorithms —

Part 7: Tweakable block ciphers

1 Scope

This document specifies tweakable block ciphers. A tweakable block cipher is a family of n -bit permutations parametrized by a secret key value and a public tweak value. Such primitives are generic tools that can be used as building blocks to construct cryptographic schemes such as encryption, Message Authentication Codes, authenticated encryption, etc.

A total of five different tweakable block ciphers are defined. They are categorized in [Table 1](#).

Table 1 — Tweakable block ciphers specified

Block length	Tweakey length	Algorithm name
128 bits	256 bits	Deoxys-TBC-256
128 bits	384 bits	Deoxys-TBC-384
64 bits	192 bits	Skinny-64/192
128 bits	256 bits	Skinny-128/256
128 bits	384 bits	Skinny-128/384

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at <https://www.iso.org/obp>
- IEC Electropedia: available at <https://www.electropedia.org/>

3.1

block

string of bits of a defined length

[SOURCE: ISO/IEC 18033-1:2021 3.5]

3.2

ciphertext

data which has been transformed to hide its information content

[SOURCE: ISO/IEC 18033-1:2021, 3.7]