Doc No. : LITD 17 (23010)
Draft IS/ISO/IEC 18033-7:2022
July 2023

BUREAU OF INDIAN STANDARDS

DRAFT FOR COMMENTS ONLY

मसौदा भारतीय मानक
सूचना सुरक्षा - एन्क्रिप्शन एल्गोरिथम - भाग 7: टिवकेबल ब्लॉक साइफर

Draft Indian Standard

Information security — Encryption algorithms — Part 7: Tweakable block ciphers

ICS 35.030

Information Systems Security and Privacy Sectional Committee, LITD 17	**Last Date for Comments: 22 Sep 20223**

NATIONAL FOREWORD

(Formal clauses will be added later)

This Draft Indian Standard (Part 7) which is identical with ISO/IEC 18033-7:2022 'Information security — Encryption algorithms — Part 7: Tweakable block ciphers' issued by International Organization for Standardization (ISO) International Electrotechnical Commission (IEC) will be adopted by the Bureau of Indian Standards on the recommendations of the Information Systems Security and Privacy Sectional Committee, LITD 17 and approval of the Electronics and Information Technology Division Council.

Other parts in this series are:
Part 1: General
Part 2:Asymmetric Ciphers

Part 3: Block Ciphers
Part 4: stream ciphers
Part 5: Identity - Based ciphers

The text of ISO Standard *may be* approved as suitable for publication as an Indian Standard without deviations. Certain conventions are however not identical to those used in Indian Standards. Attention is particularly drawn to the following:

a) Wherever the words 'International Standard' appears referring to this standard, they should be read as 'Indian Standard'.

b) Comma (,) has been used as a decimal marker while in Indian Standards, the current Practice is to use a point (.) as the decimal marker.

Scope of ISO/IEC 18033-7:2022 is as follows:

"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

"

Note: - The technical content of this document has not been enclosed as these are identical with the corresponding ISO/IEC Standard. For details please refer to ISO/IEC 18033-7:2022 or kindly contact.

Head,
Electronics & IT Department
Bureau of Indian Standards
9, B.S. Zafar Marg,
New Delhi-110002
Email: hlitd@bis.gov.in, litd17@bis.gov.in
Tele: 011-23608450