INTERNATIONAL STANDARD

ISO/IEC 18033-6

First edition
2019-05

IT Security techniques — Encryption algorithms —

Part 6: Homomorphic encryption

Techniques de sécurité IT — Algorithmes de chiffrement —

Partie 6: Chiffrement homomorphe

Reference number
ISO/IEC 18033-6:2019(E)

© ISO/IEC 2019

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2019

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
Fax: +41 22 749 09 47
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 and abbreviations **3**
5 General model for homomorphic encryption **4**
5.1 Entities 4
5.2 Key roles 4
5.3 Algorithms 4
5.4 Functional requirements 4
6 Homomorphic encryption mechanisms **5**
6.1 General 5
6.2 Exponential ElGamal encryption 5
6.2.1 General 5
6.2.2 Key generation algorithm 5
6.2.3 Encryption 5
6.2.4 Decryption 6
6.3 Paillier encryption 6
6.3.1 General 6
6.3.2 Key generation algorithm 7
6.3.3 Encryption 7
6.3.4 Decryption 7
Annex A (normative) **Object identifiers** **9**
Annex B (informative) **Numerical examples** **10**
Bibliography **17**

© ISO/IEC 2019 – All rights reserved

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).

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 http://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.

This document was prepared by Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

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

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.

© ISO/IEC 2019 – All rights reserved

Introduction

Homomorphic Encryption is a type of symmetric or asymmetric encryption that allows third parties (i.e. parties that are neither the encryptor nor the decryptor) to perform operations on plaintext data while keeping the data in encrypted form. The primary purpose of homomorphic encryption is to allow third parties to perform such computations on data while simultaneously ensuring that the confidentiality of the plaintext data is preserved. It is typically the case that homomorphic encryption schemes require the plaintext to be represented in the form of elements of a group, rather than strings of bits or bytes as is the case with most conventional methods of encryption.

Homomorphic encryption mechanisms can be categorized by the nature of the operation(s) on the plaintext that they can support. This document considers homomorphic encryption mechanisms where the plaintext operation is typically addition and/or multiplication in a prescribed group.

© ISO/IEC 2019 – All rights reserved

IT Security techniques — Encryption algorithms —

Part 6: Homomorphic encryption

1 Scope

This document specifies the following mechanisms for homomorphic encryption.

— Exponential ElGamal encryption;

— Paillier encryption.

For each mechanism, this document specifies the process for:

— generating parameters and the keys of the involved entities;

— encrypting data;

— decrypting encrypted data; and

— homomorphically operating on encrypted data.

Annex A defines the object identifiers assigned to the mechanisms specified in this document. Annex B provides numerical examples.

2 Normative references

There are no normative references in this document.

© ISO/IEC 2019 – All rights reserved