

First edition
2002-12-01

Reaffirmed as
INCITS/ISO/IEC 15946-1:2008[R2014]

Information technology — Security techniques — Cryptographic techniques based on elliptic curves —

Part 1: General

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

Partie 1: Généralités

Adopted by INCITS (InterNational Committee for Information Technology Standards) as an American National Standard.

Date of ANSI Approval: 7/7/2003

Published by American National Standards Institute,
25 West 43rd Street, New York, New York 10036

Copyright 2003 by Information Technology Industry Council (ITI).
All rights reserved.

These materials are subject to copyright claims of International Standardization Organization (ISO), International Electrotechnical Commission (IEC), American National Standards Institute (ANSI), and Information Technology Industry Council (ITI). Not for resale. No part of this publication may be reproduced in any form, including an electronic retrieval system, without the prior written permission of ITI. All requests pertaining to this standard should be submitted to ITI, 1250 Eye Street NW, Washington, DC 20005.

Printed in the United States of America

Reference number
ISO/IEC 15946-1:2002(E)



© ISO/IEC 2002

This is a preview of "INCITS/ISO/IEC 15946...". [Click here to purchase the full version from the ANSI store.](#)

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

© ISO/IEC 2002

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Second edition
2008-04-15

Information technology — Security techniques — Cryptographic techniques based on elliptic curves —

Part 1: General

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

Partie 1: Généralités

Reference number
ISO/IEC 15946-1:2008(E)



© ISO/IEC 2008

This is a preview of "INCITS/ISO/IEC 15946...". Click here to purchase the full version from the ANSI store.

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2008

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

This is a preview of "INCITS/ISO/IEC 15946...". Click here to purchase the full version from the ANSI store.

Contents

Page

Foreword.....	iv
Introduction	v
1 Scope	1
2 Terms and definitions.....	1
3 Symbols	2
4 Conventions of fields	3
4.1 Finite prime fields $F(p)$	3
4.2 Finite fields $F(p^m)$	3
5 Conventions of elliptic curves.....	4
5.1 Definition of elliptic curves.....	4
5.2 The group law on elliptic curves.....	5
5.3 Cryptographic bilinear map	5
6 Conversion functions	5
6.1 Octet string / bit string conversion: OS2BSP and BS2OSP.....	5
6.2 Bit string / integer conversion: BS2IP and I2BSP.....	5
6.3 Octet string / integer conversion: OS2IP and I2OSP	6
6.4 Finite field element / integer conversion: FE2IP _F	6
6.5 Octet string / finite field element conversion: OS2FEP _F and FE2OSP _F	6
6.6 Elliptic curve point / octet string conversion: EC2OSP _E and OS2ECP _E	7
6.7 Integer / elliptic curve conversion: I2ECP.....	8
7 Elliptic curve domain parameters and public key	8
7.1 Elliptic curve domain parameters over $F(q)$	8
7.2 Elliptic curve key generation	9
Annex A (informative) Background information on finite fields	10
A.1 Bit strings	10
A.2 Octet strings.....	10
A.3 The finite field $F(q)$	10
Annex B (informative) Background information on elliptic curves	12
B.1 Properties of elliptic curves.....	12
B.2 The group law for elliptic curves E over $F(q)$ with $p > 3$	12
B.3 The group law for elliptic curves over $F(2^m)$	16
B.4 The group law for elliptic curves over $F(3^m)$	17
B.5 The existence condition of an elliptic curve E	19
Annex C (informative) Background information on elliptic curve cryptosystems.....	21
C.1 Definition of cryptographic problems.....	21
C.2 Algorithms to determine discrete logarithms on elliptic curves.....	21
C.3 Scalar multiplication algorithms of elliptic curve points.....	22
C.4 Algorithms to compute pairings.....	24
C.5 Elliptic curve domain parameters and public key validation (optional).....	25
Bibliography	30

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. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

ISO/IEC 15946-1 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

This second edition cancels and replaces the first edition (ISO/IEC 15946-1:2002), which has been technically revised.

ISO/IEC 15946 consists of the following parts, under the general title *Information technology — Security techniques — Cryptographic techniques based on elliptic curves*:

— *Part 1: General*

— *Part 3: Key establishment*

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

Introduction

One of the most interesting alternatives to the RSA and $F(p)$ based cryptosystems that are currently available are cryptosystems based on elliptic curves defined over finite fields. The concept of an elliptic curve based public-key cryptosystem is quite simple.

- Every elliptic curve over a finite field is endowed with an addition "+" under which it forms a finite abelian group.
- The group law on elliptic curves extends in a natural way to a "discrete exponentiation" on the point group of the elliptic curve.
- Based on the discrete exponentiation on an elliptic curve, one can easily derive elliptic curve analogues of the well-known public-key schemes of the Diffie-Hellman and ElGamal type.

The security of such a public-key cryptosystem depends on the difficulty of determining discrete logarithms in the group of points of an elliptic curve. This problem is, with current knowledge, much harder than the factorisation of integers or the computation of discrete logarithms in a finite field. Indeed, since Miller and Koblitz independently suggested the use of elliptic curves for public-key cryptographic systems in 1985, the elliptic curve discrete logarithm problem has only been shown to be solvable in certain specific, and easily recognisable, cases. There has been no substantial progress in finding a method for solving the elliptic curve discrete logarithm problem on arbitrary elliptic curves. Thus, it is possible for elliptic curve based public-key systems to use much shorter parameters than the RSA system or the classical discrete logarithm based systems that make use of the multiplicative group of some finite field. This yields significantly shorter digital signatures and system parameters and the integers to be handled by a cryptosystem are much smaller.

This part of ISO/IEC 15946 describes the mathematical background and general techniques necessary for implementing any of the mechanisms described in other parts of ISO/IEC 15946 and other ISO/IEC standards.

It is the purpose of this part of ISO/IEC 15946 to meet the increasing interest in elliptic curve based public-key technology and describe the components that are necessary to implement secure elliptic curve cryptosystems such as key-exchange, key-transport and digital signatures.

The International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) draw attention to the fact that it is claimed that compliance with this document may involve the use of patents.

The ISO and IEC take no position concerning the evidence, validity and scope of these patent rights.

The holders of these patent rights have assured the ISO and IEC that they are willing to negotiate licences under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statements of the holders of these patent rights are registered with the ISO and IEC. Information may be obtained from:

ISO/IEC JTC 1/SC 27 Standing Document 8 (SD 8) "Patent Information"

SD 8 is publicly available at: <http://www.ni.din.de/sc27>

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights other than those identified above. ISO and IEC shall not be held responsible for identifying any or all such patent rights.