IEEE Standard Specification for Public Key Cryptographic Techniques Based on Hard Problems over Lattices

IEEE Computer Society

Sponsored by the
Microprocessor Standards Committee

IEEE
3 Park Avenue
New York, NY 10016-5997, USA

10 March 2009

IEEE Std 1363.1™-2008

IEEE Standard Specification for Public Key Cryptographic Techniques Based on Hard Problems over Lattices

Sponsor
Microprocessors and Microcomputers Committee
of the
IEEE Computer Society

Approved 10 December 2008

IEEE-SA Standards Board

Abstract: Specifications of common public key cryptographic techniques based on hard problems over lattices supplemental to those considered in IEEE Std 1363-2000 and IEEE Std 1363a-2004, including mathematical primitives for secret value (key) derivation, public key encryption, identification and digital signatures, and cryptographic schemes based on those primitives are provided. Also presented are specifications of related cryptographic parameters, public keys, and private keys. Class of computer and communications systems is not restricted.

Keywords: encryption, lattice-based cryptography, public key cryptography

The Institute of Electrical and Electronics Engineers, Inc.
3 Park Avenue, New York, NY 10016-5997, USA

PDF: ISBN 978-0-7381-5863-1 STD95858
Print: ISBN 978-0-7381-5864-8 STDPD95858

IEEE Standards documents are developed within the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE-SA) Standards Board. The IEEE develops its standards through a consensus development process, approved by the American National Standards Institute, which brings together volunteers representing varied viewpoints and interests to achieve the final product. Volunteers are not necessarily members of the Institute and serve without compensation. While the IEEE administers the process and establishes rules to promote fairness in the consensus development process, the IEEE does not independently evaluate, test, or verify the accuracy of any of the information contained in its standards.

Use of an IEEE Standard is wholly voluntary. The IEEE disclaims liability for any personal injury, property or other damage, of any nature whatsoever, whether special, indirect, consequential, or compensatory, directly or indirectly resulting from the publication, use of, or reliance upon this, or any other IEEE Standard document.

The IEEE does not warrant or represent the accuracy or content of the material contained herein, and expressly disclaims any express or implied warranty, including any implied warranty of merchantability or fitness for a specific purpose, or that the use of the material contained herein is free from patent infringement. IEEE Standards documents are supplied "**AS IS**."

The existence of an IEEE Standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE Standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard. Every IEEE Standard is subjected to review at least every five years for revision or reaffirmation. When a document is more than five years old and has not been reaffirmed, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE Standard.

In publishing and making this document available, the IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity. Nor is the IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing this, and any other IEEE Standards document, should rely upon the advice of a competent professional in determining the exercise of reasonable care in any given circumstances.

Interpretations: Occasionally questions may arise regarding the meaning of portions of standards as they relate to specific applications. When the need for interpretations is brought to the attention of IEEE, the Institute will initiate action to prepare appropriate responses. Since IEEE Standards represent a consensus of concerned interests, it is important to ensure that any interpretation has also received the concurrence of a balance of interests. For this reason, IEEE and the members of its societies and Standards Coordinating Committees are not able to provide an instant response to interpretation requests except in those cases where the matter has previously received formal consideration. At lectures, symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall make it clear that his or her views should be considered the personal views of that individual rather than the formal position, explanation, or interpretation of the IEEE.

Comments for revision of IEEE Standards are welcome from any interested party, regardless of membership affiliation with IEEE. Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Comments on standards and requests for interpretations should be addressed to:

Secretary, IEEE-SA Standards Board
445 Hoes Lane
Piscataway, NJ 08854
USA

Introduction

This introduction is not part of IEEE Std 1363.1-2008, IEEE Standard Specification for Public Key Cryptographic Techniques Based on Hard Problems over Lattices.

The IEEE P1363™ project started as the "Standard for Rivest-Shamir-Adleman, Diffie-Hellman, and Related Public Key Cryptography" with its first meeting in January 1994, following a strategic initiative by the Microprocessor Standards Committee to develop standards for cryptography. Over the next eight years, the working group produced a broad standard reflecting the state of the art in public key cryptography, including techniques from three major families of hard problems. In addition, the working group drafted an addendum that provides additional techniques from those three major families. A more thorough history of the IEEE P1363 working group and its contributions beyond IEEE Std 1363™-2000 are given in the Introduction to IEEE Std 1363-2000.

At the same time, new cryptographic research was producing additional families of cryptographic techniques such as the family of techniques based on hard problems over lattices. These techniques enjoy operating characteristics that make them attractive in certain implementation environments, and thus they have received considerable scrutiny and deployment.

As a result, the working group proposed a new project to standardize techniques from this family. This project was approved by the Microprocessors and Microcomputers Standards Committee, and this current standard is the result of this project.

Notice to users

Laws and regulations

Users of these documents should consult all applicable laws and regulations. Compliance with the provisions of this standard does not imply compliance to any applicable regulatory requirements. Implementers of the standard are responsible for observing or referring to the applicable regulatory requirements. IEEE does not, by the publication of its standards, intend to urge action that is not in compliance with applicable laws, and these documents may not be construed as doing so.

Copyrights

This document is copyrighted by the IEEE. It is made available for a wide variety of both public and private uses. These include both use, by reference, in laws and regulations, and use in private self-regulation, standardization, and the promotion of engineering practices and methods. By making this document available for use and adoption by public authorities and private users, the IEEE does not waive any rights in copyright to this document.

Updating of IEEE documents

Users of IEEE standards should be aware that these documents may be superseded at any time by the issuance of new editions or may be amended from time to time through the issuance of amendments, corrigenda, or errata. An official IEEE document at any point in time consists of the current edition of the document together with any amendments, corrigenda, or errata then in effect. In order to determine whether a given document is the current edition and whether it has been amended through the issuance of amendments, corrigenda, or errata, visit the IEEE Standards Association web site at http://ieeexplore.ieee.org/xpl/standards.jsp, or contact the IEEE at the address listed previously.

For more information about the IEEE Standards Association or the IEEE standards development process, visit the IEEE-SA web site at http://standards.ieee.org.

Errata

Errata, if any, for this and all other standards can be accessed at the following URL: http://standards.ieee.org/reading/ieee/updates/errata/index.html. Users are encouraged to check this URL for errata periodically.

Interpretations

Current interpretations can be accessed at the following URL: http://standards.ieee.org/reading/ieee/interp/index.html.

Patents

Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken with respect to the existence or validity of any patent rights in connection therewith. The IEEE is not responsible for identifying Essential Patent Claims for which a license may be required, for conducting inquiries into the legal validity or scope of Patents Claims or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance, if any, or in any licensing agreements are reasonable or non-discriminatory. Users of this standard are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. Further information may be obtained from the IEEE Standards Association.

Participants

At the time this standard was submitted to the IEEE-SA Standards Board for approval, the P1363 Working Group had the following membership:

William Whyte, *Chair*
Don Johnson, *Vice Chair*

Matthew Ball
Xavier Boyen
Mike Brenner
Daniel Brown
Mark Chimley
Andy Dancer
David Jablon
Satoru Kanno
David Kravitz
Michael Markowitz
Luther Martin
Jim Randall
Roger Schlafly
Ari Singer
Terence Spies
Yongge Wang

The following members of the individual balloting committee voted on this standard. Balloters may have voted for approval, disapproval, or abstention.

Ed Addario
Butch Anton
Matthew Ball
H. Stephen Berger
Martin J. Bishop
Juan Carreon
Keith Chow
Kevin Coggins
Geoffrey Darnton
James Davis
Thomas Dineen
Andrew Fieldsend
Michael Geipel
Randall Groves
Werner Hoelzl
Atsushi Ito
Mark Jaeger
Susan Land
David J. Leciston
Daniel Lindberg
Edward McCall
Avygdor Moise
Michael S. Newman
Ulrich Pohl
Robert Robinson
Randall Safier
Bartien Sayogo
Thomas Starai
Walter Struppler
Gerald Stueve
Mark Sturza
Vincent Tume
William Whyte
Paul Work
Oren Yuen
Wenhao Zhu

When the IEEE-SA Standards Board approved this standard on 10 December 2008, it had the following membership:

Robert M. Grow, *Chair*
Thomas Prevost, *Vice Chair*
Steve M. Mills, *Past Chair*
Judith Gorman, *Secretary*

Victor Berman
Richard DeBlasio
Andy Drozd
Mark Epstein
Alexander Gelman
William R. Goldbach
Arnold M. Greenspan
Kenneth S. Hanus
Jim Hughes
Richard H. Hulett
Young Kyun Kim
Joseph Koepfinger*
John Kulick
David J. Law
Glenn Parsons
Ronald C. Petersen
Chuck Powers
Narayanan Ramachandran
Jon Walter Rosdahl
Robby Robson
Anne-Marie Sahazizia
Malcolm V. Thaden
Howard L. Wolfman
Don Wright

*Member Emeritus

Also included are the following nonvoting IEEE-SA Standards Board liaisons:
Satish K. Aggarwal, *NRC Representative*
Michael Janezic, *NIST Representative*

Don Messina
IEEE Standards Program Manager, Document Development

Malia Zaman
IEEE Standards Program Manager, Technical Program Development

Contents

IEEE Standard Specification for Public Key Cryptographic Techniques Based on Hard Problems over Lattices

1. Overview

1.1 Scope

This standard provides specifications of common public key cryptographic techniques based on hard problems over lattices supplemental to those considered in IEEE Std 1363™-2000 [B47][1] and IEEE Std 1363a™-2004 [B48], including mathematical primitives for secret value (key) derivation, public key encryption, identification and digital signatures, and cryptographic schemes based on those primitives. Specifications of related cryptographic parameters, public keys, and private keys are also presented. Class of computer and communications systems is not restricted.

1.2 Purpose

The transition from paper to electronic media brings with it the need for electronic privacy and authenticity. Public key cryptography offers fundamental technology addressing this need. Many alternative public key techniques have been proposed, each with its own benefits. IEEE Std 1363-2000 [B47] and IEEE Std 1363a-2004 [B48] have produced a comprehensive reference defining a range of common public key

[1] The numbers in brackets correspond to those of the bibliography in Annex B.