ICS 35.040
CCS L 80

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 15851.3-2018

Replacing GB/T 15851-1995

Information technology -- Security techniques -- Digital signature schemes giving message recovery -- Part 3: Discrete logarithm based mechanisms

Issued on: December 28, 2018 **Implemented on: July 1, 2019**

Issued by: State Administration for Market Regulation, China National Standardization Administration

Table of Contents

Foreword

GB/T 15851 "Information Technology Security Technology with Digital Signature Scheme for Message Recovery" is currently divided into the following sections.

--- Part 2. Mechanism based on large number decomposition;

--- Part 3. Mechanism based on discrete logarithm.

This part is the third part of GB/T 15851.

This part is drafted in accordance with the rules given in GB/T 1.1-2009.

This part replaces GB/T 15851-1995 "Information Technology Security Technology with Digital Signature Scheme for Message Recovery", and

Compared with GB/T 15851-1995, the main technical differences are as follows.

--- Supplementary provisions of the key generation process;

--- In addition to the digital signature framework with message recovery, five new digital signature schemes are defined and the signature of each signature scheme is specified.

And verification method;

--- Supplementary provisions for the use of the hash function;

--- Partial signature scheme increases the use of elliptic curves or finite fields;

--- Added instructions for full and partial message recovery;

---Add a normative reference document;

--- Replace the original Appendix A and Appendix B with 8 new appendices, which are used to describe the key derivation function and the digital signature scheme.

Examples.

This section uses the redrafting method to modify the number of information security

technologies with information recovery using ISO /IEC 9796-3.2006

Word Signature Scheme Part 3. Mechanism Based on Discrete Logarithm and its Corrigendum.

This section has structural changes compared to ISO /IEC 9796-3.2006. Chapter 11 was deleted and Chapter 12 was changed to Chapter 11, Chapter 13.

Chapters were changed to Chapter 12, adding 8.3.6, 9.3.6, 10.3.6, 11.3.6 and 12.3.6.

The technical differences between this part and ISO /IEC 9796-3.2006 and their reasons are as follows.

--- Deleted Chapter 11 and its related content to match the technical level of our country.

Introduction

Digital signature mechanisms can provide entity authentication, data source authentication, non-repudiation, and data integrity services.

The digital signature mechanism satisfies the following requirements.

--- If there is only a public verification key, no private signature key, generate a valid signature for any given message in the calculation

Is not feasible;

--- The signature generated by the signing party cannot be used to generate a valid signature for a new message, nor can it be used to recover a signature.

Key

--- For signers, finding two different messages with the same signature is computationally infeasible.

Most of the signature mechanisms are based on asymmetric cryptography and consist of three basic operations.

--- the process of generating a key pair, each key pair including a private signature key and a corresponding public verification key;

--- The process of using a private signature key, called the signature generation process;

--- The process of using a public verification key is called the signature verification process.

There are two types of digital signature mechanisms.

--- For a given private signature key, the signer's signature on the same message is the same, this mechanism is called non-random (or indeed

() ISO /IEC 14888-1];

--- For each given message and a given private signature key, the signature generated by each signature process is different, this mechanism is called

It is random.

This section specifies a random digital signature mechanism.

Digital signature schemes can also be divided into the following two categories.

--- When the entire message needs to be stored and/or transmitted along with the signature, the scheme is called "signature scheme with appendix" [see ISO /

IEC 14888];

--- When the whole or part of the message can be recovered from the signature, the scheme is called "signature scheme with message recovery".

If the message is short enough, the entire message can be included in the signature and recovered from the signature by the signature verification process; otherwise a part of the message

Points can be included in the signature, and the remaining parts are stored or transmitted along with the signature. The mechanisms specified in this section provide complete or partial recovery.

The purpose is to reduce storage and transfer management.

This section includes five signature schemes. The scheme specified in this section uses a hash function to operate on the entire message. ISO /IEC

10118 specifies a hash function. Some of the schemes specified in this section use a group of elliptic curves over a finite field. ISO /IEC

15946-1.2002 describes the mathematical background and basic techniques for implementing cryptosystems based on elliptic curves over finite fields. Defined in this section

The characteristics of the mechanism are given in Appendix G. These mechanisms are related to the mechanisms defined in ISO /IEC 9796-3.2000 and ISO /IEC 15946-4.2004.

See Appendix H for correspondence.

Information technology security technology with message recovery

Digital signature scheme

Part 3. Discrete log-based mechanisms

1 Scope

This part of GB/T 15851 specifies five digital signature schemes with message recovery.

The security of these programs is based on

The difficulty of the discrete logarithm problem of elliptic curves on a finite or finite field.

This section also defines an optional control field in the hashing token that enhances the security of the signature.

This section specifies a random mechanism.

The mechanisms specified in this section are capable of restoring messages in whole or in part.

Note. The discrete logarithmic based digital signature scheme with appendix is described in ISO /IEC 14888-3.

2 Normative references

The following documents are indispensable for the application of this document. For dated references, only dated versions apply to this article.

Pieces. For undated references, the latest edition (including all amendments) applies to this document.

ISO /IEC 10118 (all parts) Information Technology Security Technology Hash Function (Informationtechnology-Security

techniques-Hash-functions)

Information technology - Security techniques - Elliptic curve based cryptographic techniques - Part 1. General

(Informationtechnology-Securitytechniques-Cryptographictechniquesbasedonelipticcurves-

Part 1.General)

Information technology - Security techniques - Elliptic curve based cryptography - Part 5. Elliptic curve generation

(Informationtechnology-Securitytechniques-Cryptographictechniquesbasedonelipticcurves-

Part 5. Elipticcurvegeneration)

3 Terms and definitions

The following terms and definitions apply to this document.

3.1

Data input datainput

Depending on the octet string of the complete message or part of the message, it forms