Chinastandards.org

ICS 35.040

GM

GM/T 0044.5-2016

Identity-based cryptographic algorithms SM9 -- Part 5: Parameter definition

SM9标识密码算法 第5部分：参数定义

(English Translation)

Issued by: State Administration of Cryptography

Preview: page 1 of 3 shown, 36 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0044-5-2016

Chinastandards.org

Table of Contents

1 Scope

2 Normative references

3 Parameter definition

3.1 System parameters

3.2 Representation of the elements of extension fields

1 Foreword

GM/T 0044.5-2016 was issued by State Administration of Cryptography on 28 March 2016.

It is one of 6 parts of the GM/T 0044 series.

The GM/T prefix marks a recommended standard. It is not law in itself: it becomes binding when a contract names it, when a regulation or a mandatory standard refers to it, or when a producer declares conformity with it.

2 Scope Preview

This part specifies the curve parameters for use with the SM9 identity-based cryptographic algorithms and provides examples for the usage of the digital signature algorithm, the key exchange protocol, the key encapsulation mechanism, and the public key encryption algorithm. This part applies to the verification of correctness in stepwise operations for the implementation of SM9 identity-based cryptographic algorithms.

GM/T 0044.5-2016 falls under ICS 35.040, in the field of information technology.

This catalogue holds 105 other GM/T standards in that field.

In this catalogue, GM/T standards carry edition years from 2012 to 2024.

3 Normative references

GM/T 0004 - , SM3 Cryptographic Hash Algorithm GM/T 0002, SM4 Block Cipher Algorithm

GM/T 0044.1 - ?2016, SM9 Identity-based Cryptographic Algorithms - Part 1: General

GM/T 0044.2 - ?2016, SM9 Identity-based Cryptographic Algorithms - Part 2: Digital Signature Algorithm

GM/T 0044.3 - ?2016, SM9 Identity-based Cryptographic Algorithms - Part 3: Key Exchange Protocol

Preview: page 2 of 3 shown, 36 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0044-5-2016

GM/T 0044.4 - ?2016, SM9 Identity-based Cryptographic Algorithms - Part 4: Key Encapsulation Mechanism and Public Key Encryption Algorithm

4 About this standard

Issued by: State Administration of Cryptography

English translation: about 36 pages

5 Related standards

Other parts of this standard:

GM/T 0044-2016 - SM9 identity-based cryptographic algorithm

GM/T 0044.1-2016 - Part 1: General

GM/T 0044.2-2016 - Part 2: Digital signature algorithm

GM/T 0044.3-2016 - Part 3: Key exchange protocol

GM/T 0044.4-2016 - Part 4: Key encapsulation mechanism and public key encryption alogorithm

6 Classification and status

International classification (ICS): 35.040

Prefix GM/T: recommended standard.

Preview: page 3 of 3 shown, 36 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0044-5-2016