Chinastandards.org

ICS 35.040

GM

GM/T 0003.1-2012

Public Key Cryptographic Algorithm SM2 Based on Elliptic Curves - Part 1: General

SM2椭圆曲线公钥密码算法 第1部分：总则

(English Translation)

Issued by: State Administration of Cryptography

Preview: page 1 of 3 shown, 77 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0003-1-2012

Chinastandards.org

Table of Contents

1 Scope
2 Symbols and abbreviations
3 Field and elliptic curve
3.1 Finite field
3.2 Elliptic curve on finite field
4 Data types and their conversion
4.1 Data type
4.2 Data type conversion
5 Elliptic curve system parameters and their verification
5.1 General requirements
5.2 System parameters of elliptic curves on Fp and their verification
5.3 System parameter of elliptic curves on and their verification
6 Key pair generation and public key verification
6.1 Key pair generation
6.2 Public key verification

1 Foreword

GM/T 0003.1-2012 was issued by State Administration of Cryptography on 21 March 2012.

It is one of 5 parts of the GM/T 0003 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 of GM/T 0003 specifies the necessary mathematical basics and related cryptographic techniques involved in public key cryptographic algorithm SM2 based on elliptic curves to help implement the cryptographic mechanisms specified in other parts. This part applies to the elliptic curve public key cryptography algorithm with the base field being the prime field and the binary extension field.

GM/T 0003.1-2012 falls under ICS 35.040, in the field of information technology.

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

Preview: page 2 of 3 shown, 77 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0003-1-2012

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

3 About this standard

Issued by: State Administration of Cryptography

English translation: about 77 pages

4 Related standards

Other parts of this standard:

GM/T 0003.2-2012 - Baded on Elliptic Curves - Part 2: Digital Signature Algorithm

GM/T 0003.3-2012 - Part 3: Key Exchange Protocol

GM/T 0003.4-2012 - Part 4: Public Key Encryption Algorithm

GM/T 0003.5-2012 - Baded on Elliptic Curves - Part 5: Parameter Definition

5 Classification and status

International classification (ICS): 35.040

Chinese Standard Classification (CCS): L 80

Prefix GM/T: recommended standard.

Preview: page 3 of 3 shown, 77 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0003-1-2012