Chinastandards.org

ICS 35.040

GM

GM/T 0003.4-2012

Public Key Cryptographic Algorithm SM2 Based on Elliptic Curves - Part 4: Public Key Encryption Algorithm

SM2椭圆曲线公钥密码算法 第4部分：公钥加密算法

(English Translation)

Issued by: State Administration of Cryptography

Preview: page 1 of 3 shown, 17 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0003-4-2012

Chinastandards.org

Table of Contents

1 Scope
2 Normative References
3 Terms and Definitions
4 Symbols
5 Algorithm Parameters and Auxiliary Functions
5.1 General
5.2 Elliptic Curve System Parameters
5.3 User Key Pair
5.4 Auxiliary Functions
5.4.1 General
5.4.2 Cryptographic Hash Function
5.4.3 Key Derivation Function
5.4.4 Random Number Generator
6 Encryption Algorithm and its Process
6.1 Encryption Algorithm
6.2 Encryption Algorithm Process
7 Decryption Algorithm and its Process
7.1 Decryption Algorithm
7.2 Decryption Algorithm Process

1 Foreword

GM/T 0003.4-2012 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 public key encryption algorithm for the public key cryptographic algorithm SM2 based on elliptic curves, and gives examples of message encryption and decryption and their corresponding processes. This part is applicable to the

Preview: page 2 of 3 shown, 17 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0003-4-2012

message encryption and decryption in the commercial cypher application, the message sender can encrypt the message with the receiver's public key and the receiver decrypts with corresponding private key to obtain the message. Meanwhile, this part also can provide standard setting and standardization reference with regard to products and technologies for security product manufacturers, and improve the credibility and interoperability of security products.

GM/T 0003.4-2012 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 0003.1-2012 - Public Key Cryptographic Algorithm SM2 Based on Elliptic Curves - Part 1: General

4 About this standard

Issued by: State Administration of Cryptography

English translation: about 17 pages

5 Related standards

Other parts of this standard:

GM/T 0003.1-2012 - Part 1: General

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

6 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, 17 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0003-4-2012