ICS 35.040
L 80
备案号:36828—2012

GM

中华人民共和国密码行业标准

GM/T 0003.3—2012

SM2 椭圆曲线公钥密码算法
第 3 部分:密钥交换协议

**Public key cryptographic algorithm SM2 based on elliptic curves—
Part 3:Key exchange protocol**

2012-03-21 发布　　2012-03-21 实施

国家密码管理局　　发 布

目　　次

前　言

GM/T 0003—2012《SM2 椭圆曲线公钥密码算法》分为 5 个部分：

——第 1 部分：总则；

——第 2 部分：数字签名算法；

——第 3 部分：密钥交换协议；

——第 4 部分：公钥加密算法；

——第 5 部分：参数定义。

本部分为 GM/T 0003 的第 3 部分。

本部分依据 GB/T 1.1—2009 给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本部分的附录 A 为资料性附录。

本部分由国家密码管理局提出并归口。

本部分起草单位：北京华大信安科技有限公司、中国人民解放军信息工程大学、中国科学院数据与通信保护研究教育中心。

本部分主要起草人：陈建华、祝跃飞、叶顶峰、胡磊、裴定一、彭国华、张亚娟、张振峰。

引　言

N. Koblitz 和 V. Miller 在 1985 年各自独立地提出将椭圆曲线应用于公钥密码系统。椭圆曲线公钥密码所基于的曲线性质如下：

——有限域上椭圆曲线在点加运算下构成有限交换群，且其阶与基域规模相近；

——类似于有限域乘法群中的乘幂运算，椭圆曲线多倍点运算构成一个单向函数。

在多倍点运算中，已知多倍点与基点，求解倍数的问题称为椭圆曲线离散对数问题。对于一般椭圆曲线的离散对数问题，目前只存在指数级计算复杂度的求解方法。与大数分解问题及有限域上离散对数问题相比，椭圆曲线离散对数问题的求解难度要大得多。因此，在相同安全程度要求下，椭圆曲线密码较其他公钥密码所需的密钥规模要小得多。

本部分描述了基于椭圆曲线的密钥交换协议。

SM2 椭圆曲线公钥密码算法
第 3 部分:密钥交换协议

1 范围

GM/T 0003 的本部分规定了 SM2 椭圆曲线公钥密码算法的密钥交换协议,并给出了密钥交换与验证示例及其相应的流程。

本部分适用于商用密码应用中的密钥交换,可满足通信双方经过两次或可选三次信息传递过程,计算获取一个由双方共同决定的共享秘密密钥(会话密钥)。同时,本部分还可为安全产品生产商提供产品和技术的标准定位以及标准化的参考,提高安全产品的可信性与互操作性。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

GM/T 0003.1—2012 SM2 椭圆曲线公钥密码算法 第 1 部分:总则

3 术语和定义

下列术语和定义适用于本文件。

3.1

从 A 到 B 的密钥确认 key confirmation from A to B

使用户 B 确信用户 A 拥有特定秘密密钥的保证。

3.2

密钥派生函数 key derivation function

通过作用于共享秘密和双方都知道的其他参数,产生一个或多个共享秘密密钥的函数。

3.3

发起方 initiator

在一个协议的操作过程中发送首轮交换信息的用户。

3.4

响应方 responder

在一个协议的操作过程中不是发送首轮交换信息的用户。

3.5

可辨别标识 distinguishing identifier

可以无歧义辨别某一实体身份的信息。

4 符号

下列符号适用于本部分。

A,B:使用公钥密码系统的两个用户。