国密SM2算法研究报告

作者：王秦豫

2017.07

[1 背景 1](#_Toc29885)

[2 概念 1](#_Toc1160)

[2.1 算法概述 1](#_Toc24160)

[2.2 算法原理 2](#_Toc2724)

[2.3 算法适用领域 2](#_Toc6177)

[2.4 相关算法 3](#_Toc14776)

[3 对比 3](#_Toc13309)

[3.1 SM2算法与RSA算法对比 3](#_Toc12423)

[3.1.1原理对照 3](#_Toc8075)

[3.1.2安全对照 3](#_Toc28807)

[3.1.3 性能对照 4](#_Toc32680)

[3.2 SM2的局限性 5](#_Toc30586)

# 1 背景

RSA1024是世界ISO推荐使用的公钥数据加密标准，它能够被用作数据加密/解密、签名认证，多年来抵抗了绝大多数的密码攻击行为。受到大家的一致认可。

原则上，只要RSA的秘钥长度足够长，就可以抵御任何密码攻击。据统计，1991年人们已经破解了100位长度的RSA-100，2003年美国密码协会发表已经能够制造破解秘钥长度为1024位的RSA-1024，RSA实验室立即修正了国际推荐值，根据预测，1024位的RSA密码只应适用到2010年，2048位的RSA密码只应适用到2030年，3072位RSA密码只应适用到2030年。秘钥长度的增长速度越来越快。随着全球密码技术和计算机技术的提高，尤其是分布式的计算和量子计算机的问世，现有的RSA1024密码体系早已经不能满足社会的基本需求。但是国内大部分公司还都使用着过时的RSA-1024，只有部分公司使用最新推荐的RSA-2048。我国政府为了国家信息安全和国防需求，在2010年12月由国家密码管理局下发规定，使用全新的SM2椭圆曲线密码算法的公钥密码信息系统，并同时给出了SM3密码杂凑算法予以配合。

# 2 概念

## 2.1 算法概述

SM2椭圆曲线公钥密码算法是由国家密码管理局于2010年12月发布，该算法属于有限域上离散对数问题，该问题主要研究在多倍点运算中，已知多倍点与曲线基点，求倍率的数值。因为该问题的求解极其困难，所需时间和计算度非常巨大，因此此问题所引出的算法适合作为密码算法。该算法在短时间（如1000年内）无法被快速破解，所以在国内被认为是当前可以替代RSA-1024算法的最优算法。根据《SM2椭圆曲线公钥加密算法》，该算法所描述的椭圆曲线具有以下性质：

Def 1 : 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。

Def 2 : 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。

## 2.2 算法原理

SM2椭圆曲线公钥算法是基于ECC算法的基础，并固定算法所涉及的曲线方程及必要参数。利用基点的不同倍率可以得到不同点值单向性的特点，把曲线映射为加密算法，将倍率定为私钥，将结果值定为公钥。

## 2.3 算法适用领域

SM2椭圆曲线公钥算法可以用于以下方面：

1. 数字签名、验签
2. 加密、解密
3. 密钥协商

## 2.4 相关算法

1. SM1，对称加密算法，加密强度为128位，采用硬件实现。
2. SM3，密码杂凑算法，杂凑值长度为32字节，和SM2算法同期公布。
3. SM4，对称加密算法，随WAPI标准一起公布，可使用软件实现，加密强度为128位。

# 3 对比

## 3.1 SM2算法与RSA算法对比

### 3.1.1原理对照

|  |  |  |
| --- | --- | --- |
|  | RSA算法 | SM2算法 |
| 问题所属 | 大数因子分解问题 | 有限域离散对数问题 |
| 计算结构 | 基于特殊的可逆模幂运算 | 基于椭圆曲线 |

### 3.1.2安全对照

|  |  |  |
| --- | --- | --- |
|  | RSA算法 | SM2算法 |
| 计算复杂度 | 亚指数级 | 完全指数级 |
| 破解难度 | 中等 | 困难 |
| 相同安全性能下所需要秘钥位数 | 较多 | 较少 |

两个算法在不同密钥长度下的现状：

RSA-512已被破解，RSA-768已被破解，RSA-1024已可作出破解机器，岌岌可危。

SM2-106已被破解，SM2-132已被破解。

因此，在相同秘钥长度下，SM2算法的抗攻击能力更强，安全性更高；在相同安全强度下，SM2算法的秘钥占据的储存空间更小。

### 3.1.3 性能对照

|  |  |  |
| --- | --- | --- |
|  | RSA算法 | SM2算法 |
| 秘钥生成速度 | 慢 | 快 |
| 加解密速度 | 一般 | 较快 |

著名的Certicom实验已经证明，在相同安全强度下，ECC（SM2核心）运算速度比RSA快一个数量级。

抽取检验签名：

|  |  |  |
| --- | --- | --- |
| 算法 | 签名速度（次/秒） | 验签速度（次/秒） |
| 1024位RSA | 2792 | 51224 |
| 2048位RSA | 455 | 15122 |
| 256位SM2 | 4095 | 871 |

## 3.2 SM2的局限性

1. 由中国政府领导的国家密码管理局发布的算法，不具有世界通用性，不具备OID标识符，其次给出了秘钥长度和曲线参数推荐值，这些值不兼容其他国家的相关算法，推荐值同样不具备OID标识符。
2. 算法难度大，产品少。

# 4 产品

## 4.1 开源产品

### 4.1.1 GmSSL

（1）产品介绍

GmSSL是一个开源的密码工具箱，支持SM2/SM3/SM4/SM9等国密(国家商用密码)算法、SM2国密数字证书及基于SM2证书的SSL/TLS安全通信协议，支持国密硬件密码设备，提供符合国密规范的编程接口与命令行工具，可以用于构建PKI/CA、安全通信、数据加密等符合国密标准的安全应用。GmSSL项目是OpenSSL项目的分支，并与OpenSSL保持接口兼容。因此GmSSL可以替代应用中的OpenSSL组件，并使应用自动具备基于国密的安全能力。GmSSL项目采用对商业应用友好的类BSD开源许可证，开源且可以用于闭源的商业应用。GmSSL项目由北京大学关志副研究员的密码学研究组开发维护，项目源码托管于GitHub。自2014年发布以来，GmSSL已经在多个项目和产品中获得部署与应用，并获得2015年度“一铭杯”中国Linux软件大赛二等奖(年度最高奖项)与开源中国密码类推荐项目。GmSSL项目的核心目标是通过开源的密码技术推动国内网络空间安全建设。官方网站：http://gmssl.org/

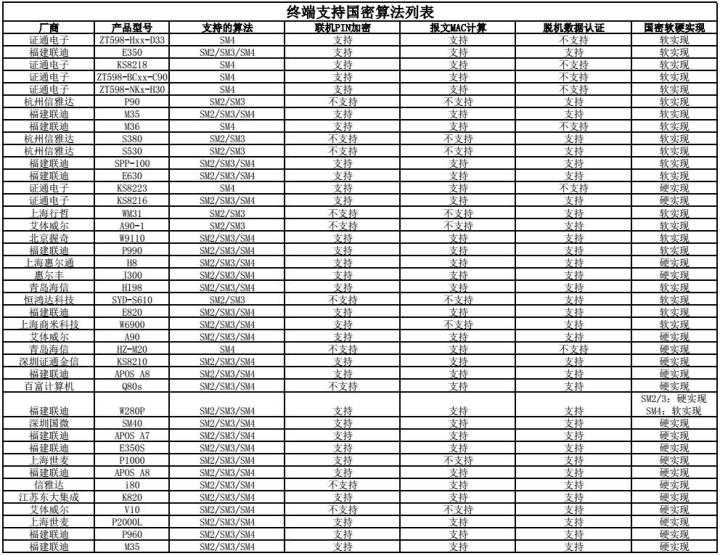
1. 产品使用



1. API支持

GmSSL Java Wrapper是GmSSL密码库接口的Java语言封装，提供了包括随机数生成、对称加解密、哈希、消息认证码(MAC)、公钥加解密、数字签名、密钥交换等基础密码功能的Java语言接口，支持包括SM2/SM3/SM4/RSA/AES/3DES/MD5/SHA-1/SHA-2在内的GmSSL密码库的全部密码算法。GmSSL Java Wrapper是GmSSL项目的子项目，用于支持Java和Android平台上的应用开发。其他语言的支持有：EVP、PHP、Go

## 4.2 商用产品



## 4.3芯片产品（来源于网络信息）

1. 广州中盈物流
2. 同方股份有限公司生产的TF32A09安全芯片