SM2 椭圆曲线公钥密码算法

国家密码管理局于 2010 年 12 月 17 日发布了 SM2 椭圆曲线公钥密码算法，并要求为对现有基于 RSA 算法的电子认证系统、密钥管理系统、应用系统进行升级改造。关于算法标准，请参见《国家密码管理局公告（第 21 号）》，网址为 http://www.oscca.gov.cn/。

SM2 算法是一种什么样的加密算法，有什么特点，如何进行应用？本文整理在 SM2 应用实践中遇到的问题，供大家分享。

SM2 算法和 RSA 算法的关系

SM2 算法和 RSA 算法都是公钥密码算法，SM2 算法是一种更先进安全的算法，在我们国家商用密码体系中被用来替换 RSA 算法。

为何要采用 SM2 算法替换 RSA 算法

随着密码技术和计算技术的发展，目前常用的 1024 位 RSA 算法面临严重的安全威胁，我们国家密码管理部门经过研究，决定采用 SM2 椭圆曲线算法替换 RSA 算法。SM2 算法在安全性、性能上都具有优势，参见表 1 算法攻破时间，表 2 算法性能。

RSA 密钥强度	椭圆曲线密钥强度	攻破时间(年)
512	106	10^4,已被攻破
768	132	10^8,已被攻破
1024	160	10^{11}
2048	210	10^{20}

表 1 算法攻破时间

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

表 2 算法性能

SM2 和椭圆曲线算法是的关系

一提起曲线，大家就会想到方程，椭圆曲线算法是通过方程确定的，SM2 算法采用的椭圆曲线方程为：

$$y2 = x3 + ax + b$$

在 SM2 算法标准中，通过指定 a、b 系数，确定了唯一的标准曲线。同时，为了将曲线映射为加密算法，SM2 标准中还确定了其它参数，供算法程序使用。

椭圆曲线算法的原理

本文不探讨椭圆曲线的数学理论，仅通过图示展示算法原理。请参见下图：

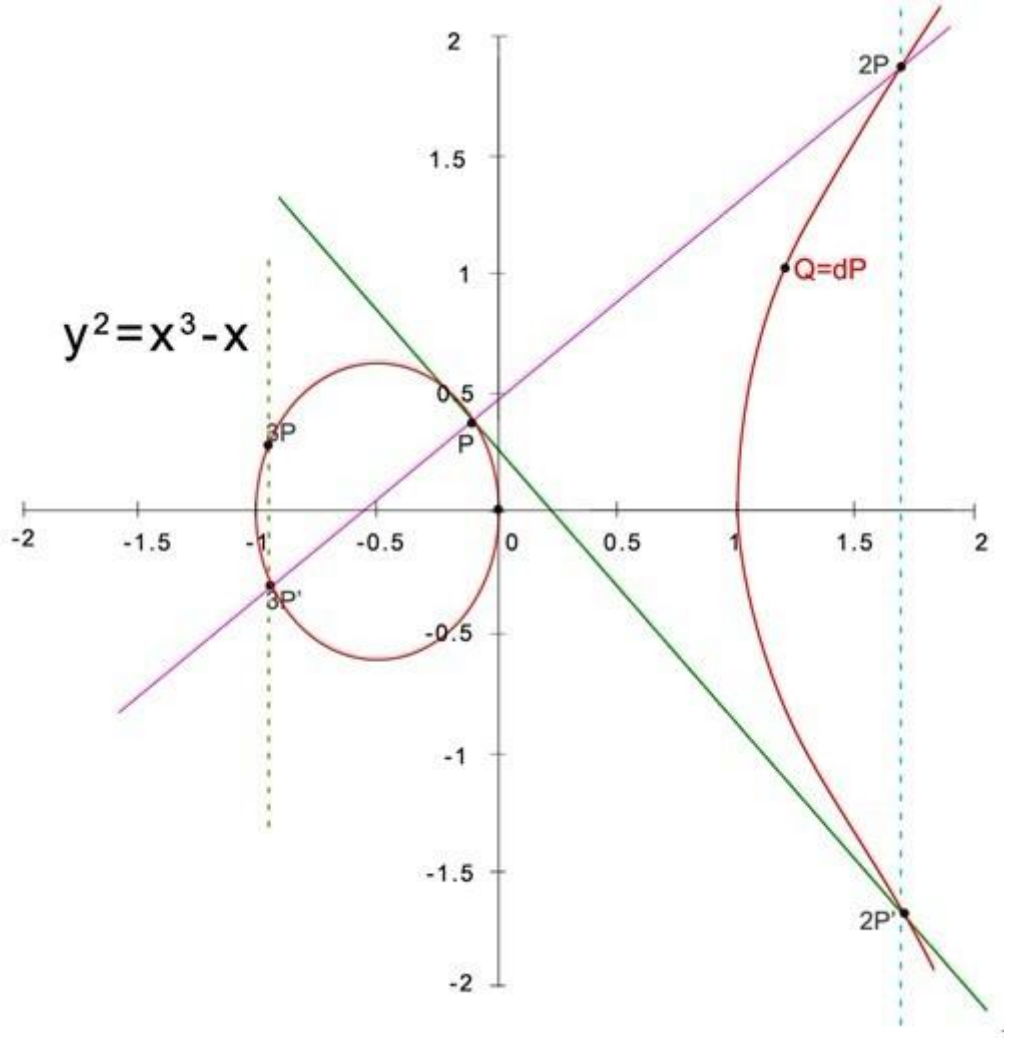

图 1 椭圆曲线算法原理

上图为方程：y2 = x3–x 的曲线。

1、P 点为基点；

2、通过 P 点做切线，交与点 2P 点，在 2P’ 点做竖线，交与 2P 点，2P 点即为 P 点的 2 倍点；

3、进一步，P 点和 2P 点之间做直线，交与 3P’ 点，在 3P’ 点做竖线，交与 3P 点，3P 点即为 P 点的 3 倍点；

4、同理，可以计算出 P 点的 4、5、6、… 倍点；

5、如果给定图上 Q 点是 P 的一个倍点，请问 Q 是 P 的几倍点呢？

6、直观上理解，正向计算一个倍点是容易的，反向计算一个点是 P 的几倍点则困难的多。

在椭圆曲线算法中，将倍数 d 做为私钥，将 Q 做为公钥。当然，椭圆曲线算法还有更严格的计算过程，相对图示要复杂的多。

SM2 算法可以进行的密码应用

SM2 算法做为公钥算法，可以完成签名、密钥交换以及加密应用。SM2 算法标准确定了标准过程：

1、签名、验签计算过程；

2、加密、解密计算过程；

3、密钥协商计算过程。

需要说明，其他国家的标准和 SM2 确定的计算过程存在差异，也就是说相互之间是不兼容的。

SM2 算法的速度

简单讲，SM2 签名速度快，验签速度慢，这点和 RSA 算法的特性正好相反。参见表 2。

另外，加解密速度和验签速度相当。

SM2 签名算法支持多大的数据量，签名结果为多少字节？

签名原始数据量长度无限制，签名结果为 64 字节。

SM2 加密算法支持多大的数据量，加密结果增加多少字节？

支持近 128G 字节数据长度，加密结果增加 96 个字节。

SM2 相关算法有哪些？

SM2 为国家密码管理局公布的公钥算法，其加密强度为 256 位。其它几个重要的商用密码算法包括：

SM1，对称加密算法，加密强度为 128 位，采用硬件实现；

SM3，密码杂凑算法，杂凑值长度为 32 字节，和 SM2 算法同期公布，参见《国家密码管理局公告（第 22 号）》；

SMS4，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。