

# 有关基于离散对数算法 的密码的建议： 椭圆曲线域参数

内部资料

翻译：高卓

Lily Chen

Dustin Moody

Andrew Regenscheid

信息技术实验室计算机安全部

Karen Randall

Randall 咨询公司

本出版物英文版可从以下网址免费获得：

<https://doi.org/10.6028/NIST.SP.800-186-draft>

2019 年 10 月



美国商务部

Wilbur L. Ross Jr., 部长

国家标准和技术研究所

Walter Copan, 商务部副部长兼 NIST 所长

北京江南天安科技有限公司

# 目录

## 执行摘要

### 第 1 章 介绍

- 1.1 背景
- 1.2 目的和范围
- 1.3 篇章结构

### 第 2 章 术语表、符号和缩略语

- 2.1 术语表
- 2.2 符号和缩略语

### 第 3 章 椭圆曲线概述

- 3.1 非二进制曲线
  - 3.1.1 短 Weierstrass 形式曲线
  - 3.1.2 Montgomery 曲线
  - 3.1.3 扭曲的 Edwards 曲线
- 3.2 二进制曲线
  - 3.2.1 短 Weierstrass 形式曲线

### 第 4 章 建议可用于美国联邦政府的曲线

- 4.1 密钥长度、底层域、曲线和基点的挑选
  - 4.1.1 密钥长度的挑选
  - 4.1.2 底层域的挑选
  - 4.1.3 二进制域基的挑选
  - 4.1.4 曲线的挑选
  - 4.1.5 基点的挑选
- 4.2 素域上的曲线
  - 4.2.1 Weierstrass 曲线
  - 4.2.2 Montgomery 曲线
  - 4.2.3 扭曲的 Edwards 曲线
- 4.3 二进制域上的曲线
  - 4.3.1 Koblitz 曲线
  - 4.3.2 伪随机曲线

## 参考文献

### 附录 A 椭圆曲线群运算详述

- A.1 非二进制曲线
  - A.1.1 Weierstrass 曲线的群运算法则
  - A.1.2 Montgomery 曲线的群运算法则
  - A.1.3 扭曲的 Edwards 曲线的群运算法则
- A.2 二进制曲线
  - A.2.1 Weierstrass 曲线的群运算法则

### 附录 B 不同曲线模型之间的关系

- B.1 扭曲的 Edwards 曲线与 Montgomery 曲线之间的映射
- B.2 Montgomery 曲线与 Weierstrass 曲线之间的映射

B.3 扭曲的 Edwards 曲线与 Weierstrass 曲线之间的映射

B.4 四同源映射

## 附录 C 建议的椭圆曲线的生成详述

C.1 密码总则

C.1.1 执行方案的安全准则

C.2 曲线生成细节

C.2.1 素域上定义的 Weierstrass 曲线

C.2.2 Montgomery 曲线

C.2.3 扭曲的 Edwards 曲线

C.2.4 二进制域上定义的 Weierstrass 曲线

C.3 伪随机曲线的生成和验证

C.3.1 伪随机曲线的生成（素数曲线）

C.3.2 曲线的伪随机性验证（素数曲线）

C.3.3 伪随机曲线的生成（二进制曲线）

C.3.4 曲线的伪随机性验证（二进制曲线）

## 附录 D 有关椭圆曲线的常规流程

D.1 公钥验证

D.1.1 短 Weierstrass 形式的非二进制曲线

D.1.2 Montgomery 曲线

D.1.3 扭曲的 Edwards 曲线

D.1.4 短 Weierstrass 形式的二进制曲线

D.2 点压缩

D.2.1 短 Weierstrass 形式的素数曲线

D.2.2 短 Weierstrass 形式的二进制曲线

D.3 基点（生成器）的挑选

D.3.1 基点的生成

D.3.2 可验证随机性的基点

D.3.3 基点的有效性

## 附录 E 辅助函数

E.1 求二进制域平方根

E.2 解二进制域方程  $x^2 + x = w$

E.3 求非二进制域  $GF(q)$  平方根

E.4  $GF(q)$  求逆

## 附录 F 数据转换

F.1 域元素转换成整数

F.2 整数转换成域元素

F.3 整数转换成位串

F.4 位串转换成整数

## 附录 G 执行的各个方面

G.1 模运算的执行

G.1.1 曲线 P-224

G.1.2 曲线 P-256

G.1.3 曲线 P-384

- G.1.4 曲线 P-512
- G.1.5 曲线 Curve448
- G.1.6 曲线 Curve25519
- G.2 Koblitz 曲线的标量乘运算
- G.3 二进制域的多项式基和正规基
  - G.3.1 正规基
  - G.3.2 从多项式基到正规基的转换
  - G.3.3 从正规基到多项式基的转换
- 附录 H 其他被允许使用的椭圆曲线**
  - H.1 Brainpool 曲线