

<<椭圆曲线密码快速算法理论>>

图书基本信息

书名：<<椭圆曲线密码快速算法理论>>

13位ISBN编号：9787115289438

10位ISBN编号：7115289433

出版时间：2012-10

出版时间：人民邮电出版社

作者：丁勇

页数：166

字数：245000

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

## <<椭圆曲线密码快速算法理论>>

### 内容概要

《椭圆曲线密码快速算法理论》以作者及其研究组多年的研究成果为主体，结合国内外专家及学者在椭圆曲线密码快速算法方面的代表性成果，系统论述了这一领域的主要研究内容。

本书分为两个部分，共7章。

第一部分(第1、2章)讲述了研究椭圆曲线密码体制所需的基础知识及椭圆曲线上点的计算；第二部分(第3~7章)讲述了椭圆曲线密码的快速算法及其分析，主要包括非邻接形式(NAF)的改进形式，基于最大公约数(GCD)算法的高速带模除法，基于多基表示的快速算法，基于双基数链的Tate对优化算法。

《椭圆曲线密码快速算法理论》既可以作为密码学、信息安全、计算机科学等相关专业的研究生教学参考书，也可作为教师和相关科研人员的参考书。

# <<椭圆曲线密码快速算法理论>>

## 书籍目录

### 第1章 椭圆曲线密码简介

- 1.1 无穷远点
- 1.2 数论相关概念
  - 1.2.1 同余和剩余类的概念
  - 1.2.2 euler定理和中国剩余定理
- 1.3 有限域简介
- 1.4 椭圆曲线简介
  - 1.4.1 椭圆的概念
  - 1.4.2  $gf(p)$ 上的椭圆曲线群
  - 1.4.3  $gf(2^m)$ 上的椭圆曲线
  - 1.4.4 ecc的困难问题
  - 1.4.5 ecdsa算法
- 1.5 ecc的安全性分析
- 1.6 总结

### 第2章 ecc上的点计算及几种常见的算法

- 2.1 点计算算法即计算量分析
- 2.2 射影坐标
- 2.3 总结

### 第3章 基于非邻接形式(naf)的快速算法

- 3.1 w-nnaf表示
  - 3.1.1 引言
  - 3.1.2 naf和nafw
  - 3.1.3 w-nnaf表示
  - 3.1.4 w-nnaf分析
  - 3.1.5 总结
- 3.2 koblitz曲线上的多比特组合方法
  - 3.2.1 引言
  - 3.2.2 solinas方法
  - 3.2.3 多比特组合方法
  - 3.2.4 总结
- 3.3 rtsnaf方法
  - 3.3.1 引言
  - 3.3.2 rtsnaf方法
  - 3.3.3 总结
- 3.4 -naf窗口技术
  - 3.4.1 引言
  - 3.4.2 自同态
  - 3.4.3 -naf分解
  - 3.4.4 -naf窗口技术
  - 3.4.5 总结
- 3.5 窗口3naf的联合稀疏形式
  - 3.5.1 引言
  - 3.5.2 jsf表示
  - 3.5.3 wt-jsf
  - 3.5.4 总结

## <<椭圆曲线密码快速算法理论>>

### 3.6 通用的 -naf分解方法

#### 3.6.1 引言

#### 3.6.2 通用 -naf分解

#### 3.6.3 总结

### 第4章 jsf与frobenius映射的结合

#### 4.1 引言

#### 4.2 lee等的方法

##### 4.2.1 frobenius表示

##### 4.2.2 方法1

##### 4.2.3 方法2

#### 4.3 与jsf的结合

#### 4.4 总结

### 第5章 基于gcd算法的高速带模除法

#### 5.1 引言

#### 5.2 常规gcd算法

#### 5.3 改进的gcd算法

#### 5.4 gcd算法的扩展

##### 5.4.1 a. zadeh的扩展

##### 5.4.2 新算法的扩展

#### 5.5 数值运算结果

#### 5.6 总结

### 第6章 基于双基表示的快速算法

#### 6.1 引言

#### 6.2 半点运算

#### 6.3 双基数字系统(db)

#### 6.4 改进的双基表示与半点方法

##### 6.4.1 extend db 方法

##### 6.4.2 双基链和半点方法

##### 6.4.3 提出的算法

##### 6.4.4 数值运算结果

##### 6.4.5 总结

#### 6.5 基于半点与多基表示的快速标量乘算法

##### 6.5.1 多基表示

##### 6.5.2 新的标量表示及标量乘算法

##### 6.5.3 数值运算结果

##### 6.5.4 总结

### 第7章 基于双基数链的tate对优化算法

#### 7.1 引言

#### 7.2 双线性对

##### 7.2.1 扭转点

##### 7.2.2 有理函数

##### 7.2.3 零点和极点

##### 7.2.4 除子

##### 7.2.5 tate对

##### 7.2.6 tate对的miller算法

##### 7.2.7 tate对的计算实例

#### 7.3 基于双基数链的tate对优化算法

## <<椭圆曲线密码快速算法理论>>

7.4 算法7.3的复杂度分析

7.4.1 tdbl的计算

7.4.2 ttrl的计算

7.4.3 tdbl\_add的计算

7.4.4 tdbl\_sub的计算

7.4.5 ttrl\_add的计算

7.4.6 ttrl\_sub的计算

7.5 算法之间复杂度比较

7.6 总结

附录

参考文献

## <<椭圆曲线密码快速算法理论>>

### 编辑推荐

涉及具体技术算法细节及相关程序多年研究积累，反映该领域最新成果作者多年密码学和信息安全研究经验

<<椭圆曲线密码快速算法理论>>

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>