

# 《基于配对的密码学》

## 图书基本信息

书名：《基于配对的密码学》

13位ISBN编号：9787030404068

出版时间：2014-4

作者：李发根,吴威峰

页数：246

版权说明：本站所提供下载的PDF图书仅提供预览和简介以及在线试读，请支持正版图书。

更多资源请访问：[www.tushu000.com](http://www.tushu000.com)

# 《基于配对的密码学》

## 内容概要

《基于配对的密码学》可供密码学与信息安全领域的科研人员参考，也可以作为密码学、信息安全、计算机、通信工程等专业的研究生教学用书。

## 书籍目录

前言

第1章引言

1.1研究背景

1.2椭圆曲线密码体制

1.2.1实数域上的椭圆曲线

1.2.2有限域上的椭圆曲线

1.2.3椭圆曲线上的ElGamal加密体制

1.3双线性配对理论

1.4困难问题

1.5公钥认证方法

参考文献

第2章PBC库

2.1PBC的使用

2.1.1PBC的安装

2.1.2配置开发环境

2.1.3执行配对运算

2.1.4进一步说明

2.2配对操作函数

2.2.1配对类型

2.2.2初始化函数

2.2.3运算函数

2.2.4其他函数

2.3元素操作函数

2.3.1初始化函数

2.3.2运算函数

2.3.3输入和输出函数

2.3.4其他函数

2.4辅助函数

2.4.1随机数函数

2.4.2动态数组函数

2.4.3设置配对参数函数

2.5PBC的组织结构

2.6常用密码操作实验

参考文献

第3章基于配对的加密体制

3.1公钥加密体制

3.2随机预言模型与标准模型

3.3基于身份的加密体制

3.3.1形式化模型

3.3.2BF体制

3.3.3Waters体制

3.3.4算法实现

3.3.5性能分析

3.4无证书加密体制

3.4.1形式化模型

3.4.2AP体制

3.4.3算法实现

## 3.4.4性能分析

### 参考文献

## 第4章基于配对的签名体制

### 4.1数字签名体制

#### 4.2短签名体制

##### 4.2.1BLS体制

##### 4.2.2ZSS体制

##### 4.2.3BB体制

##### 4.2.4算法实现

##### 4.2.5性能分析

### 4.3基于身份的签名体制

#### 4.3.1形式化模型

##### 4.3.2CC体制

##### 4.3.3Hess体制

##### 4.3.4BLMQ体制

##### 4.3.5PS体制

##### 4.3.6算法实现

##### 4.3.7性能分析

### 4.4无证书签名体制

#### 4.4.1形式化模型

##### 4.4.2AP体制

##### 4.4.3ZWXF体制

##### 4.4.4算法实现

##### 4.4.5性能分析

### 参考文献

## 第5章基于配对的组合密码体制

### 5.1组合密码体制

### 5.2基于身份的组密码体制

#### 5.2.1形式化模型

##### 5.2.2具体实例

##### 5.2.3算法实现

##### 5.2.4性能分析

### 参考文献

## 第6章基于配对的密钥协商协议

### 6.1一轮三方密钥协商协议

### 6.2基于身份的密钥协商协议

#### 6.2.1Smart协议

#### 6.2.2Shim协议

### 6.3无证书密钥协商协议

#### 6.4协议实现

#### 6.5性能分析

### 参考文献

## 第7章基于配对的不可否认认证协议

### 7.1可否认认证协议

### 7.2基于身份的可否认认证协议

#### 7.2.1形式化模型

##### 7.2.2LXJ协议

##### 7.2.3协议实现

##### 7.2.4性能分析

参考文献

# 《基于配对的密码学》

## 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:[www.tushu000.com](http://www.tushu000.com)