分 类 号: TP309,TN918　　密　级:

论文编号: 2015010008

贵 州 大 学

2019届博士研究生学位论文

理性隐私保护模型及应用

学科专业: 应用数学

研究方向: 密码学与数据安全

导　　师: 向淑文、彭长根

研 究 生: 丁红发

中国·贵州·贵阳

2019年 9月

目　录

摘　　要

TBC

关键词： 隐私保护，博弈论，隐私量化，隐私推测，基于风险访问控制

Abstract

TBC

Keywords: Privacy preserving, Game Theory, Privacy quantification, Privacy inference, Risk adaptable based access control

第一章　绪论

1.1　研究背景及意义

1.2　研究现状

1.2.1　理性隐私保护研究概况

1.2.2　隐私保护算法

1.2.3　隐私攻击与推测

1.2.4　隐私量化

1.3　有待解决的关键问题

1.4　本文工作

1.5　论文结构

第二章　基础知识

2.1　Shannon信息论及其扩展

2.1.1　熵

2.1.2　互信息

2.2　结构信息论

2.2.1　博弈论

2.2.2　博弈模型

2.2.3　策略博弈

2.2.4　扩展博弈

2.2.5　演化博弈

2.3　隐私定义及隐私保护

2.3.1　隐私

2.3.2　演化博弈

第三章　基于信息通信模型的隐私度量模型

第四章　基于结构信息论的隐私量化模型

第五章　相互独立的序列型数据的隐私属性推测模型及其应用

第六章　相互关联的序列型数据的隐私属性推测模型及其应用

第七章　面向隐私保护的风险自适应访问控制模型

第八章　理性的隐私风险访问控制模型及其分析

第九章　总结及展望

9.1　结论

9.2　展望

参考文献

致　　谢

致谢

攻读博士学位期间科研和论文情况

一、科研工作

主持科研项目：

1. 贵州大学研究生创新基金：大数据环境下的风险自适应隐私保护访问控制模型及其应用研究(No.研理工2016068)

参与科研项目：

1. 国家自然科学基金重点项目：数据共享应用的块数据融合分析理论与安全管控模型研究(No. U1836205)
2. 国家自然科学基金地区项目：理性隐私计算及隐私风险可控技术研究(No. 61662009)
3. 国家自然科学基金面上项目：理性委托计算的可组合安全理论及其构造方法研究(No.61772008)
4. 贵州省科技计划重大专项：面向多源法院数据融合的数据安全防护与隐私保护算法及模型研究(No. 黔科合重大专项字[2017]3002)
5. 贵州省科技计划重大专项：大数据安全与隐私保护关键技术研究(No. 黔科合重大专项字[2018]3001)

二、发表论文

[1] **Ding Hongfa**, Peng Changgen, Tian Youliang and Xiang Shuwen. A risk adaptive access control model based on Markov for big data in the cloud, International Journal of High Performance Computing and Networking, 2019, 13(4):464-475.(**EI**)

[1] 彭长根,**丁红发**,朱义杰,田有亮,符祖峰.隐私保护的信息熵模型及其度量方法[J].软件学报,2016,27(08):1891-1903.(**EI，一级学报，CCF推荐A类中文期刊**)

[2] 刘波涛,彭长根,吴睿雪,**丁红发**,谢明明.面向数字型的轻量级保形加密算法研究[J].计算机研究与发展,2019,56(07):1488-1497.(**EI, 一级学报，CCF推荐A类中文期刊**)

[3] 彭长根,田有亮,刘海,**丁红发**.密码学与博弈论的交叉研究综述[J].密码学报,2017,4(01):1-15.(**CCF推荐C类中文期刊**)

[4] 谢明明,彭长根,吴睿雪,**丁红发**,刘波涛.结构化数据的隐私与数据效用度量模型[J].计算机应用研究:1-6[2019-08-25].(**CCF推荐C类中文期刊**)

二、专利

[1]**丁红发**,彭长根,朱义杰. 基于位置景区电子讲解服务的系统[P]. 贵州：CN205029878U, 2016-02-10.

[2]**丁红发**,彭长根,朱义杰. 基于位置景区电子讲解服务的系统的设计方法及系统[P]. 贵州：CN105025442A,2015-11-04.

[3]刘波涛,彭长根,吴睿雪,谢明明,**丁红发**,袁文书,夏宗涛,杨炳钊. 一种可恢复的保留数字类型轻量级脱敏方法[P]. 贵州：CN109039586A,2018-12-18.

[4]彭长根,吴睿雪,刘波涛,**丁红发**,谢明明. 具有隐私保护功能的快递实名认证方法[P]. 贵州：CN108833351A,2018-11-16.

[5]谢明明,彭长根,刘波涛,吴睿雪,**丁红发**. 一种基于传统分组密码的保持格式加密方法[P]. 贵州：CN108768617A,2018-11-06.

[6]彭长根,刘波涛,吴睿雪,谢明明,**丁红发**,李雪松. 一种基于手机身份的验证码短信透明加密方法[P]. 贵州：CN108599944A,2018-09-28.

[7]刘波涛,彭长根,吴睿雪,李雪松,**丁红发**,谢明明. 加解密一致的SP网络结构轻量级LBT分组密码实现方法[P]. 贵州：CN107707343A,2018-02-16.

附：贵州大学学位论文原创性声明和使用授权声明

原 创 性 声 明

本人郑重声明：所呈交的学位论文，是本人在导师的指导下，独立进行研究所取得的成果。除文中已经注明引用的内容外，本论文不包含任何其他个人或集体已经发表或撰写过的科研成果。对本文的研究在做出重要贡献的个人和集体，均已在文中以明确方式标明。本人在导师指导下所完成的学位论文及相关的职务作品，知识产权归属贵州大学。本人完全意识到本声明的法律责任由本人承担。

论文作者签名：_____ 日　期：_____年　月　日

关于学位论文使用授权的声明

本人完全了解贵州大学有关保留、使用学位论文的规定，同意学校保留或向国家有关部门或机构送交论文的复印件和电子版，允许论文被查阅和借阅；本人授权贵州大学可以将本学位论文的全部或部分内容编入有关数据库进行检索，可以采用影印、缩印或其他复制手段保存论文和汇编本学位论文。

本学位论文属于：

保　密（　），在_____年解密后适用授权。

不保密（　）

（请在以上相应方框内打“√”）

论文作者签名：_____导师签名：_____

日 期：_____年　月　日