贵 州 大 学

2019届博士研究生学位论文

(详细摘要)

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12月

理性隐私保护模型及应用

详细摘要

互联网、移动互联网和物联网快速发展，以及5G技术的不断推进和商用推广，社交网络、位置服务、医疗健康、生物基因、工业控制等海量数据被主动或被动采集、传输、存储、流转、分析并应用。海量数据的产生和应用推动了云计算、大数据和边缘计算等新兴产业和技术的爆发式增长，并产生了智慧医疗、智慧交通、智慧政府、智慧城市等不同的应用，极大地丰富了人们的物质和精神生活。同样，数据海量化增长、网络跨域泛在、计算云端化、应用多样复杂化等新的变化为安全和隐私带来了巨大挑战，大量的病毒、漏洞、攻击和数据关联分析，致使隐私严重泄漏，引发了人们极大的担忧。近年来主要的各类重大隐私泄露事件，充分表明了隐私泄露已经成为网络空间的重要威胁。在此背景下，深入的理解隐私并保护隐私变得尤为重要。

由于90%以上的数据被提供公共服务的政府、社会组织和企业所采集、存储，为了使数据发挥更大的价值，往往需要对包含大量隐私信息的数据进行共享、开放、交换和分析处理；同时很多信息服务也是基于个人隐私信息与服务质量的交换，如网站注册服务、公共WIFI接入、云存储、智能手机导航、信息搜索与广告推送、在线信用卡支付、RFID应用等。这些场景中由于法律法规要求和个人意愿，需要对隐私信息进行保护，同时服务提供方、数据利用方或恶意第三方希望获取更多的隐私敏感信息，以提供更好的服务、获取更大数据价值，得到更好的数据效用，两个目标同时存在且相互冲突，需要均衡解决。

关于隐私的研究，自2006年*k*匿名模型被提出以后逐步变成系统化的研究，隐私研究发展为基于密码学的方案和基于非密码学的方案两大类，这些方案被大规模应用于以数据为中心的开放、复杂、跨域场景中，如云存储、社交网络、基于位置服务、物联网、边缘计算、数据挖掘、机器学习、医疗健康等。众多应用场景中，隐私保护目标和数据利用目标天然矛盾，如何平衡二者的关系是核心问题之一。在这两类隐私研究中，基于密码学的方案通常利用可证明安全理论定义密码学意义上的隐私保护目标，设计对应的密码学方案，如同态加密、可搜索加密、属性密码方案等实现隐私保护目标。基于非密码学的方案主要是定义了匿名性设计达到匿名化效果的算法来实现用户的身份匿名隐私保护；通过定义邻近数据集的查询结果不可区分性，设计加噪的方法达到这种不可区分性来实现属性值的隐私保护；通过定义数据动态隐私，设计自适应的风险的细粒度访问控制实现隐私数据不被非授权用户访问。其中，基于密码学的方

案具有严格的理论方法支撑，能够达到预期的隐私保护目标，但是这些隐私定义是密码学意义上安全性定义，隐私保护方案设计也依赖公钥密码，其计算高度复杂导致效率低下，且难以采用折中的措施实现隐私保护效果和数据效用的平衡；基于非密码学的方案通过概率或信息论定义匿名性和不可区分性意义上的隐私，并设计泛化匿名或加噪的方式实现匿名或属性值隐私保护，效率高且有利于平衡隐私保护效果和数据效用。目前，以数据为中心的开放应用场景多样化，特别是数据开放共享应用中，大规模的个人隐私需要在保证数据可用的前提下得到实用性的隐私保护，研究基于非密码学的方案可以达到这一目标，平衡隐私保护与数据效用，具有重要的现实意义。

隐私领域的研究主要有三方面科学问题。**第一、隐私定义与度量**。如何恰当形式化的定义隐私、并对隐私进行量化。特别是隐私量化，既包括对特定数据集中隐私量的量化，又包括在某种隐私分析攻击模型下，个人隐私潜在泄露量、隐私分析攻击后隐私泄露量评估，还包括某一隐私保护模型对数据集隐私保护强度的量化。**第二、隐私分析与推断**。在某一场景下针对保护后的隐私信息数据集进行隐私分析与推断，如何最大程度的获取更多隐私信息。**第三、隐私保护**。如何对某一场景下的隐私数据集进行有效隐私保护，如何在保护隐私的同时平衡隐私保护效果和数据效用。深入研究科学问题一和科学问题二有助于对隐私的理解和认识，能够对隐私泄露的机理进行深入剖析，能够对设计更好的隐私保护方案提供科学理论依据和评价方法，研究科学问题三能够实现对数据隐私的预期性保护，如可量化的、动态性的及自适应的隐私保护，能够平衡隐私保护效果与数据效用间的关系。上述三个科学问题对基于非密码学的方案研究有重要的理论意义，能够有助于该领域完善其基础理论体系，可在保证其实用性基础上提高隐私定义形式化及度量、隐私泄露机理、隐私保护方案的科学性。

面对上述隐私领域的主要科学问题挑战，本文主要针对数据开放共享场景下的基于非密码学隐私研究领域，展开隐私度量、隐私分析、隐私保护，以及隐私保护与数据效用平衡方面研究，旨在能够深入探究隐私基础理论，提高对隐私泄露及隐私保护机理的理解，以提出能够动态、自适应地对包含大量隐私信息的数据集进行隐私保护，并实现隐私保护与数据效用间的平衡。

本文以国家自然科学基金项目《理性隐私计算及隐私风险可控技术研究》为支撑，主要聚焦在以信息论通信模型及其扩展工具研究隐私度量的基础性框架模型，能够对隐私定义、隐私分析攻击模型和隐私保护机制进行量化；以概率推断为工具建立序列型隐私数据的属性隐私分析敌手模型，并针对真实数据进行分析推断攻击，量化敌手

隐私分析攻击强度；因风险访问控制模型为基础，定义并量化风险隐私，设计动态自适应访问控制模型；以博弈论为工具，刻画访问控制隐私保护机制参与者的隐私和数据效用需求的理性行为和有限理性行为，设计能动态平衡隐私保护和数据效用关系的理性风险访问控制隐私保护机制。研究体系如图 1所示，具体取得了如下6方面的成果。

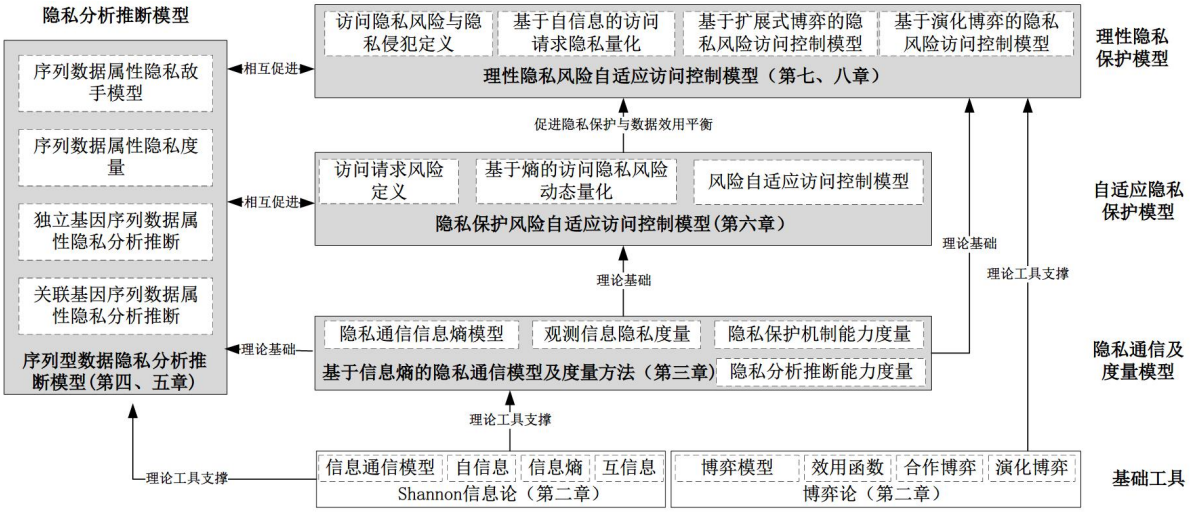

图 1: 研究体系及论文结构安排

1. 基于信息熵的隐私通信模型及度量方法

利用信息论的相关工具，如熵、互信息等来对匿名隐私、成员关系隐私和属性隐私进行形式化定义和度量的研究较多，但是大部分是集中在位置匿名、轨迹匿名、数据集匿名、数据集成员属性、训练集关系隐私、社交网络匿名和属性等方面的研究。在隐私量化方面，缺乏对隐私定义、隐私分析、隐私保护等统一的量化方法。

本文基于Shannon信息论的通信模型框架提出了几种隐私保护信息通信模型，对不含敌手的隐私保护、含敌手的隐私保护、多隐私保护源的隐私保护等不同情境提出了相应的模型进行建模，以满足对隐私度量、隐私保护机制效果度量和敌手隐私分析强度度量等需求。在所提出的度量模型中，将信息拥有者假设为发送方，隐私谋取者假设为接收方，隐私的泄露渠道假设为通信信道；基于该假设，分别引入信息熵、平均互信息量、条件熵及条件互信息等来分别描述隐私保护系统信息源的隐私度量、隐私泄露度量、含背景知识的隐私度量及泄露度量，形成了以信息论为核心的隐私度量方法体系；以此为基础，进一步提出了隐私保护方法的强度和敌手攻击强度的量化，为隐私泄露的量化提供了一种支撑，对整个隐私保护过程中的保护机制、敌手能力都提供了量化方法。

在构建的隐私保护通信模型中，将含敌手的隐私保护机制构建了如图 2所示的通信模型，并定义了信源熵、攻击条件熵、互信息量等来量化隐私。

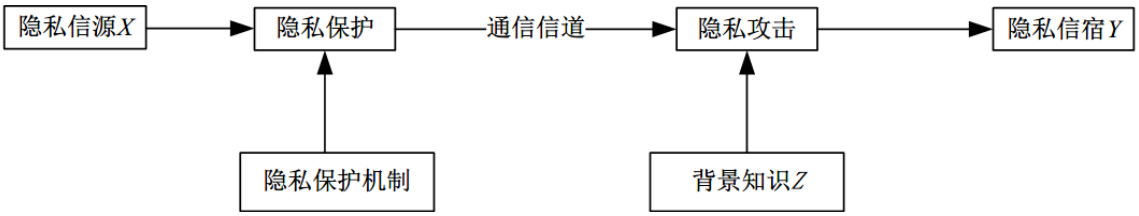

图 2: 单隐私信源且敌手具备知识背景的隐私保护通信模型

针对该模型，隐私信源熵$H(X)$为

$$H(X) = -\sum_{i=1}^{n} p(x_i)\log_2 p(x_i) \tag{1}$$

$H(X)$ 用于刻画隐私信源的平均隐私信息量，也是隐私信源的隐私不确定程度， $H(X)$ 越大，隐私泄露就可能越小，从而它亦可以用于衡量隐私的保护程度，在没有外部条件影响时，该值是一个确定的值。

隐私攻击条件熵$H(X/YZ)$为

$$H(X/YZ) = \sum_{i=1}^{n}\sum_{j=1}^{m}\sum_{k=1}^{l} p(x_i y_j z_k)\log_2 p(x_i/y_j z_k) \tag{2}$$

$H(X/YZ)$ 反映了攻击者在获得隐私信宿消息 Y 和背景知识 Z 后，关于 X 仍存在的不确定度，它实际了可以作为在具有攻击分析的情况下隐私信息的不确定度，亦可以作为隐私保护强度的度量。

隐私攻击平均互信息 $I(X;Y/Z)$ 为

$$I(X;Y/Z) = \sum_{i=1}^{n}\sum_{j=1}^{m}\sum_{k=1}^{l} p(x_i y_j z_k)\log_2 \frac{p(x_i z_k/y_j)}{p(x_i/z_k)p(y_j/z_k)} \tag{3}$$

该公式反映了得到 Z 的条件下， X 和 Y 之间的平均互信息量，即接收方获得的隐私信息量，即可以刻画具有背景知识攻击下的隐私泄露程度。

在此基础上定义了隐私保护机制、隐私分析敌手攻击能力的量化方法，具体有：

对同一隐私信源 X ，其与隐私信宿 Y 进行通信过程中受到敌手应用隐私攻击进行攻击 A_r ，系统分别应用隐私保护机制 P_i 和 P_j 对隐私消息进行保护，若

$H_{P_i,A_r}(X/YZ) < H_{P_j,A_r}(X/YZ)$ ($I_{P_i,A_r}(X;Y/Z) < I_{P_j,A_r}(X;Y/Z)$)，则称在抗 A_r 攻击下，隐私保护机制 P_j 比隐私保护机制 P_i**隐私保护有效性好**,简记偏序关系 $P_i(A_r) \prec P_j(A_r)$ 。若 $H_{P_i,A_r}(X/YZ) = H_{P_j,A_r}(X/YZ)$ ($P_{P_i,A_r}(X;Y/Z) = I_{P_j,A_r}(X;Y/Z)$)，则称隐私保护机制 P_i 与隐私保护机制 P_j**隐私保护有效性**相等，简记等价关系 $P_i(A_r) \cong P_j(A_r)$ 。

在含敌手攻击的隐私保护信息熵模型中，对同一隐私信源 X ，针对该信源的隐私消息有隐私攻击 A_r ，若在该隐私攻击下分别应用隐私保护机制 P_i 和 P_j 进行保护，隐私信源 Y 在该攻击下接收到的隐私信息量分别为 $I_{P_i,A_r}(X;Y/Z)$ 和 $I_{P_j,A_r}(X;Y/Z)$ ，则称两种隐私保护机制在隐私攻击 A_r 下的有效性距离为 $D_i(A_r) = \left|I_{P_i,A_r}(X;Y/Z) - I_{P_j,A_r}(X;Y/Z)\right|$ 。

对同一隐私信源 X ，其与隐私信宿 Y 进行通信过程中应用隐私保护机制 p_i 进行隐私保护，并分别受到敌手应用隐私攻击 A_r 和 A_α 进行攻击，若 $H_{P_i,A_r}(X/YZ) < H_{P_i,A_q}(X/YZ)$ $(I_{P_i,A_r}(X;Y/Z) > I_{P_i,A_q}(X;Y/Z)$)，则称在隐私保护机制的保护下，隐私攻击 A_r 比隐私攻击 A_α 的隐私攻击有效性更强，简记偏序关系。若 $H_{P_i,A_r}(X/YZ) < H_{P_i,A_q}(X/YZ)$ ($I_{P_i,A_r}(X,Y/Z) < I_{P_i,A_q}(X,Y/Z)$)，则称在隐私保护机制 P_i 的保护下，隐私攻击 A_r 与隐私攻击 A_α 的**隐私攻击有效性相同**,简记等价关系 $A_r(P_i) \cong A_q(P_i)$ 。

在含敌手攻击的隐私保护信息熵模型中，对同一隐私信源 X 的隐私消息应用隐私保护机制 P_i 进行保护，并有隐私攻击 A_r 和 A_α 分别进行隐私攻击，隐私信源 Y 在不同攻击下接收到的隐私信息量分别为 $I_{P_i,A_r}(X;Y/Z)$ 和 $I_{P_i,A_q}(X;Y/Z)$ ，则称两种隐私攻击针对隐私保护机制 P_i 的有效性距离为$D_i(P_i) = \left|I_{P_i,A_r}(X;Y) - I_{P_i,A_q}(X;Y)\right|$。

2. 独立序列型数据属性隐私推断模型

近年来，由于数据种类繁多、数量庞大且应用需求多样化，越来越多的数据被以集中或分布式的形式共享、开放，造成了大量的隐私泄露，这些泄露又成为敌手进行隐私分析的背景知识，增加了数据共享的隐私泄露风险，对数据隐私泄露的潜在威胁量化，对数据隐私保护机制设计都提出了高的要求。特别是需要对隐私泄露的原理进行进一步研究，以帮助更好地度量隐私、理解隐私泄露机理，并设计更好的隐私保护方法。目前针对匿名方法的去匿名性分析研究较多，针对社交网络的用户偏好、个人信息等属性隐私的分析研究较多，但是对新型序列化数据的属性隐私，如时间序列的位置隐私、基因序列的基因座敏感值隐私较少，此类数据在很多共享应用场景（如疾病诊断、车联网导航）中需要非匿名化，需要对其敏感的属性隐私（特定基因座的基因型，特定行车位置）进行保护。

本文针对基因序列数据的属性隐私提出了一种基于概率推断的隐私分析模型。该模型通过对单条敏感数据记录属性值存在的相互关联关系进行分析，构建目标属性值推断的敌手模型。在提出的敌手模型基础上，分别提出了两种不同的基因序列属性隐私分析方法。第一种主要基于Monte Carlo-Markov抽样和隐Markov推断算法，建立了目标基因序列的“抽样解析”——“单倍体属性值概率推断”——“二倍体合成”三个步骤的属性隐私推断模型；第二种方法应用卷积神经网络构建概率推断算法，改进了单倍体属性值推断过程，实现了大规模序列型数据的属性推断目标。所提出的方法针对不存在亲属关系的群体基因序列数据共享场景，在本文提出的隐私度量模型基础上，定义了序列型数据属性隐私和量化方法，并应用于分析属性隐私泄露情况，通过量化隐私泄露量和敌手获取隐私量等信息，提高对序列型数据属性隐私的认识和理解。实验表明，本文提出的方法比现有基因序列属性隐私分析模型和算法更优，敌手对属性隐私的错误率、不确定度降低，敌手获得隐私信息量都比已有的工作更优。

在所提出的序列型数据属性隐私推断模型中，提出了如图 3 所示的敌手模型。由于隐私保护的需求，被攻击者希望隐藏某些可能与遗传病或私人特征有关的敏感SNP。因此，被攻击对象共享其原始SNP序列的变体 $\hat{X}=(\hat{x}_1,\hat{x}_2,...,\hat{x}_n)$ ，其中 $\hat{x}_i=\{0,1,2\}$ ，并隐藏其中某些SNP。假设隐藏的SNP用 X_h 表示，可观测的SNP用 X_O 表示，公开的SNP用 $X=(x_1,x_2,...,x_n)=X_H\cup X_O$ ，其中 $X_i=\{-1,0,1,2\}$ ，值 $X_i=-1$ 表示 $X_i\in X_h$ 是隐藏的SNP。假设已观测被攻击者公开SNP X 序列数据的敌手想要重构原始SNP序列 $\hat{X}$ 。为此，敌手可以通过推断攻击获取被攻击者的基因组隐私（例如获得其APOE基因状态）。要进行这样的推断攻击，敌手将收集一些公开可用的基因组信息，例如被攻击者所属族群的次要等位基因频率（Minor Allele Frequency，MAF）、LD值、遗传重组率和单倍体基因型参照。

在此敌手模型下，基因序列数据属性隐私推断攻击可以看作是给定已发布的SNP和公开基因组信息，计算每个隐藏SNP的条件边缘概率分布的过程，即

$$Prob(X=\{0,1,2\})=Prob(X|(X_O,INFOR_{Pub})). \tag{4}$$

基于iHMM的隐私序列数据隐私分析攻击可以分三个步骤进行，即

(1) 敌手根据观测到的被攻击者的基因型数据，随机产生 H_V^T 的单倍型。然后，敌手通过多轮Markov链Monte Carlo迭代更新 H_V^T 中的单倍型。在每次迭代中，敌手通

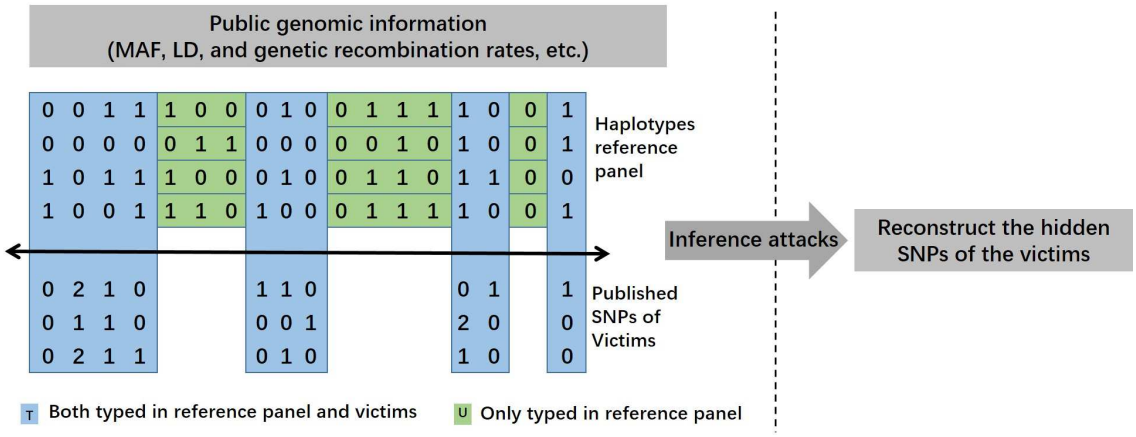

图 3: 基因序列数据属性隐私分析推断敌手模型概览

过从 $p(H_{V,i}^{T}|G_{V,i}^{T},H_{V,-i}^{T},H_{R}^{T},\rho)$ 中抽样来更新第 i 个被攻击者的阶段性单倍型对 $H_{V,i}^{T}$ 。

(2) 敌手通过基因重组模型利用HMM模型推断 H_{V}^{u} 中的单倍型。在每次迭代中，敌手根据条件概率分布 $p(H_{V,i}^{U}|H_{V,i}^{T},H_{R}^{T\cup U},\rho)$ 推断第 i 个被攻击者对应 U 中的SNP序列的隐藏单倍型对 $H_{V,i}^{u}$ 。

(3) 敌手把对每个被攻击者推断出来的单倍型对组合起来，得到被攻击者隐藏的SNP序列的推断基因型。

基于RCNN的序列型数据属性隐私推断攻击，可将上述过程的步骤（2），改变为如图4所示神经网络训练与推测过程。

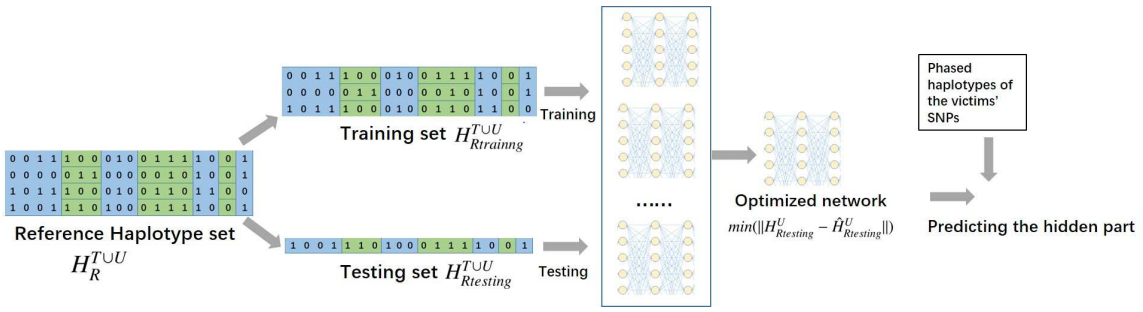

图 4: 基于RCNN的隐私分析模型

通过实验结果分析，提出的两种隐私分析攻击方法，敌手能够准确、低不确定性和高隐私损失地推断出个体的私有隐藏SNP隐私信息。所提出的攻击扩展并显著改进了现有的工作。通过基于公开的基因组数据对个体基因组隐私进行量化，本章的工作

可以帮助人们更好地理解当前基因组隐私面临的风险，促进隐私领域更加小心地应用基因组数据，促进研究人员设计更好的隐私保护模型（如后文研究的基于风险访问控制模型）以适应性地保护基因序列数据隐私。

3. 关联序列型数据属性隐私推断模型

随着不同机构和个人更加容易获取基因组数据，且这些敏感数据被广泛地应用于医疗、保险、寻亲及社交等场景，对数据安全和隐私的担忧也在不断加剧。为了证实在序列型数据属性隐私方面，存在个人共享基因数据也会大量泄漏他人属性隐私的问题，为了进一步分析家族成员基因序列数据共享会造成他人基因序列属性隐私泄露的机理，需要对相互关联的基因序列型数据进行隐私分析。

本文利用因子图和置信传播算法针对亲属间的基因序列属性隐私建立分析推断敌手模型和分析算法。该模型考虑了单核苷酸多态性间高阶相关性，利用公开DNA参照数据集和全基因组关联研究(GWAS)目录数据，提高了推断攻击模型的属性隐私分析强度。该模型的敌手隐私分析强度通过本文所提出的隐私度量框架，对基因序列属性隐私进行了定义，并将隐私损失量作为评价指标进行了隐私分析强度量化。实验结果表明，所提出的攻击更适合于高密度基因组数据隐私推断，且具有较少的错误率、不确定性和更多隐私损失，显著提高了属性隐私的隐私分析推断能力。

所提出的敌手模型中敌手的目的是通过使用(i) 观测到的一个或多个家庭成员的基因组数据(即SNP序列)，(ii) 观测到的一个或多个家庭成员的基因组相关特征和疾病，(iii) 家族的谱系结构，(iv) 遗传规律，特别是孟德尔遗传定律，(v) 核苷酸的次要等位基因频率(MAF) 或等位基因频率，(vi) SNP之间的族群LD值，(vii) 族群的SNP，(viii) GWAS目录，以及(ix) 遗传疾病的发病率等信息，推断被攻击者的SNP，身体特征和疾病。属性隐私分析框架如图5 所示。

若将家庭成员 i 的SNP j 的边缘分布表示为 $p(x_{ij})$，则 $\mathbf{X}_u$ 的每个变量的边缘概率分布可以得到为

$$p(x_{ij}) = \sum_{\mathbf{X}_U/\{x_{ij}\}} p(\mathbf{X}_U|\mathbf{X}_K, \mathbf{T}_K, \mathbf{D}_K, T, \mathscr{F}_T(x_i^F, x_i^M, x_i^C), \mathbf{P}, \mathbb{T}, \mathbb{D}, \mathbb{P}, \mathbf{F}) \tag{5}$$

我们为概率推断计算建立一个因子图以提高实际隐私分析算法计算效率。该图具有两种类型的节点（变量节点和因子节点）和连接节点的边。在此因子图中设置了每个SNP $x_{i,j}$ 的变量节点（ $x_{i,j} \in \mathbf{X}$， i 表示家庭成员ID， j 表示家庭成员 i 的SNP ID）。

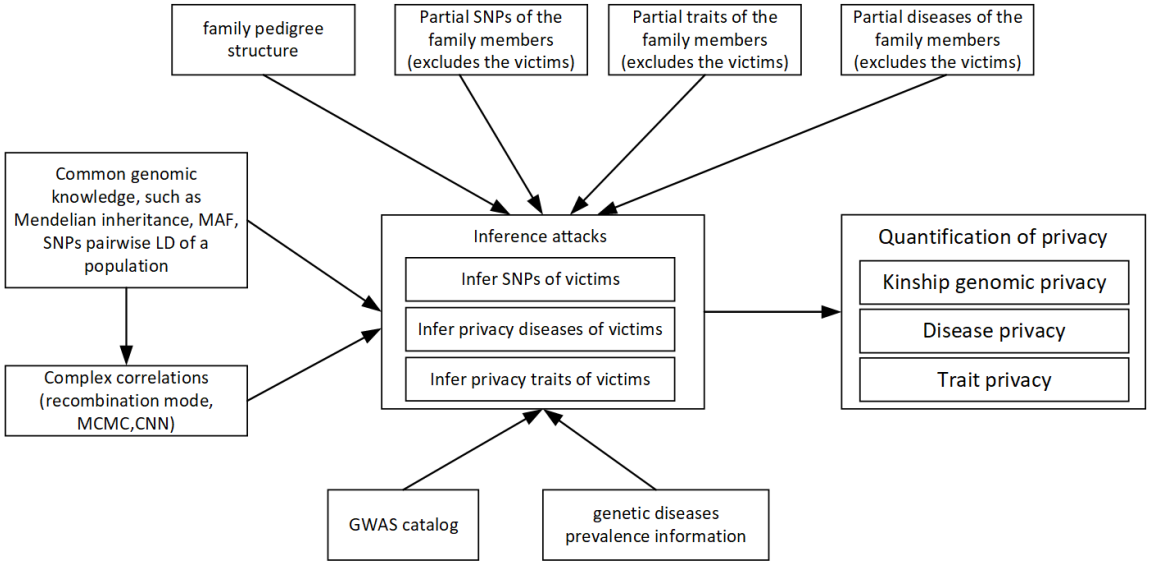

图 5: 亲属基因组属性隐私分析推断框架

本模型使用四种类型的因子节点：（i）家族因子节点，代表家族关系（关于孩子和父母）和遗传，（ii）重组模型相关因子节点，代表SNP之间的重组模型相关性，它比其他类型的高阶相关性包含更多的信息，（iii）特征因子节点代表SNP与个体特征之间的关系，以及（iv）疾病因子节点，代表SNP与个体基因组疾病之间的关系。

4. 隐私保护风险自适应访问控制模型

在以数据为中心的开放系统中，数据往往通过云服务或其他集中式的方式按需提供数据共享、开放、应用服务，这些需求多样复杂产生了复杂的隐私泄露风险和威胁，需要动态化、细粒度、适应性的方案对数据提供访问控制模式的隐私保护。但目前基于传统的强制访问控制、基于角色访问控制以及新型的基于属性访问控制，都不能很好的解决该问题。

本文针对云环境中共享、应用涉及隐私或敏感信息数据的场景研究面向隐私保护的访问控制模型。在XACML上扩展提出了一种基于风险的自适应访问控制模型，以动态化地在访问控制过程中保护数据隐私，约束隐私侵犯行为，激励诚实访问行为。首先，根据风险访问控制场景的隐私保护需求提出了面向隐私保护的风险访问控制敌手模型；其次，该模型在标准的XACML框架进行了扩展，新增了策略风险评估、会话控制和风险消减服务三个组件，增强了策略执行、策略访问和策略信息组件。在新增的组件中，以Shannon信息熵作为工具，在提出的隐私度量模型基础上，提出了基于风险的隐私定义和量化方法，对用户的访问控制请求风险和用户自身的风险类型结合，提出了访问请求类型判别方法；通过风险隐私量化及基于信用卡模型的激励机制，实现

访问行为风险阈值的动态调整，考虑了用户短期访问行为和长期访问行为的影响。对比和分析表明，所提出的模型和方法较现有的工作更加动态化，且实现了隐私保护，易用性更好。

在所提出的隐私保护访问控制模型中，其主要组件和流程如图6所示。

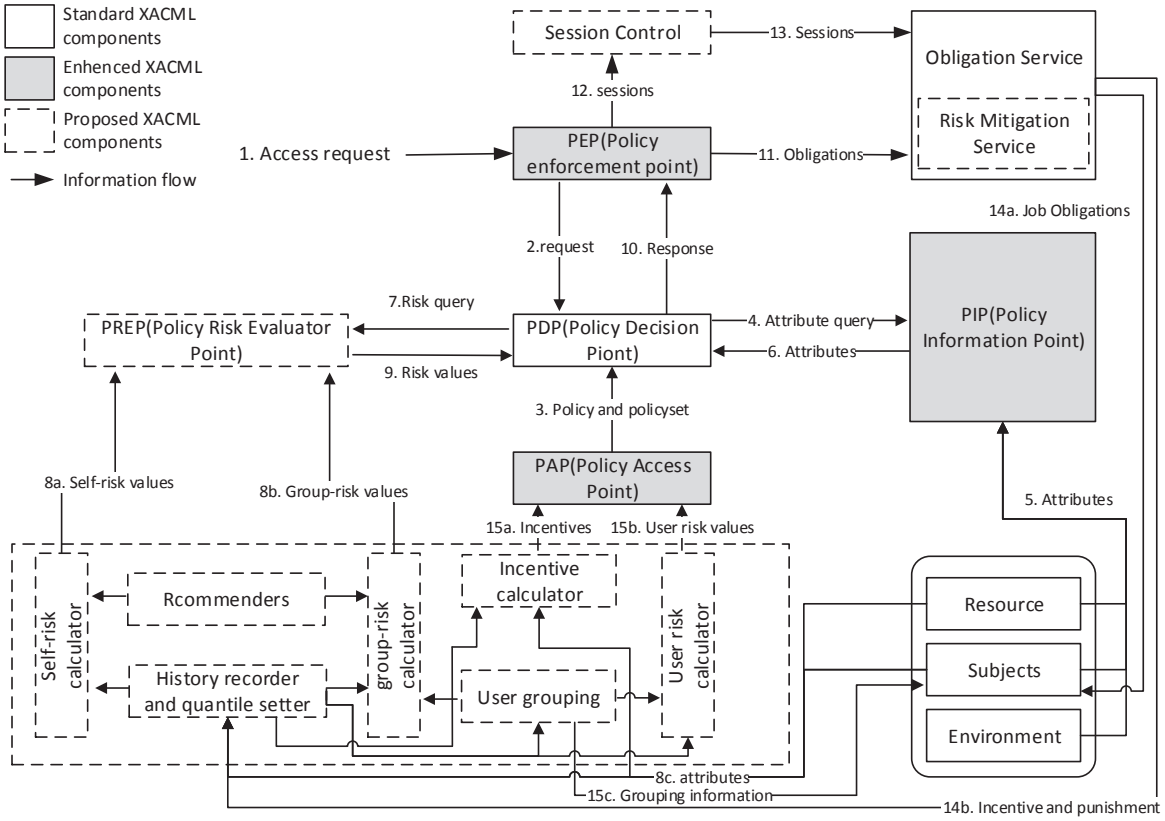

图 6: 基于XACML的风险自适应访问控制框架流程

其中，用户u的第n次访问请求q_n的自访问风险值可表示为

$$sr(u,q_n)=\begin{cases} I(q_i)=-logp_i, & \text{是否有足够的历史数据;} \\ Avg(I(u,q)), & \text{若历史还不够;} \\ 1, & \text{若没有可用的历史数据。} \end{cases} \tag{6}$$

用户u的第m次访问请求q_n的组访问风险值 $gr(g,q_m)$ 可计算为

$$gr(g,q_m)=\begin{cases} I(q_i)=-logp_i, & \text{若有足够的历史数据;} \\ Avg(I(g,q)), & \text{若历史数据不够;} \\ 1, & \text{若没有可用的历史数据。} \end{cases} \tag{7}$$

数据服务提供者或系统可以根据请求的风险级别做出访问控制决策，即

$$decision = \begin{cases} p, & \text{若 } q \text{ 为自正常访问请求，且为群组正常访问请求;} \\ p(rm), & \text{若 } q \text{ 为自风险访问请求，但为群组正常访问请求;} \\ d, & \text{若 } q \text{ 为自风险访问请求，且为群组风险访问请求;} \\ d(p), & \text{若 } q \text{ 为自正常访问请求，但为群组风险访问请求。} \end{cases} \tag{8}$$

5. 基于扩展式博弈的理性隐私风险访问控制模型

基于风险访问控制模型可很好的解决以数据为中心的开放系统中自适应数据隐私保护。但强制访问控制、基于角色访问控制、基于属性访问控制和已有的基于风险访问控制等模型，在平衡隐私保护需求与数据效用需求冲突方面，仍存在问题，特别是过度授权导致隐私泄露或授权不足导致数据可用性不足的问题需要进一步解决。此外，还需要对基于风险访问模型中对隐私保护的能力和方法进一步提升。

针对上述需求和问题，本文在所提出的风险自适应访问控制模型的基础上，进一步运用Shannon自信息和博弈论，提出了基于风险适应性的理性访问控制模型以实现数据共享场景中的保护隐私和数据应用需求间的平衡。在定义了隐私风险和隐私侵犯访问的概念之后，提出了基于博弈论的风险访问控制模型框架和工作流程，其中模型框架如图7所示。此外，还进一步利用Shannon信息的定义提出了量化访问请求隐私风险和用户隐私风险值的计算公式，强化了访问控制请求对数据隐私的刻画；以提出的理性风险访问控制模型、访问请求隐私风险和用户隐私风险为基础，提出了多轮二人博弈来刻画面向隐私保护的风险访问控制中访问者与数据服务提供者的“隐私保护-数据服务”冲突与合作关系，进一步提出并分析了博弈效用函数及其二人博弈过程。分析表明，在基于隐私风险访问控制的每一轮博弈中都存在子博弈精炼纳什均衡，可以通过限制侵犯隐私的访问请求来保护隐私，实现隐私保护与数据访问效用间的平衡。分析和对比表明，该方法比已有的工作更有优势，需要更少的辅助信息，提供更多的风险适应性和隐私保护强度。

该模型中，通过使用 r_{q_U} 的自信息和 r_i^g 的平均信息之间的距离来量化访问请求隐私风险 r_{q_U}，如下

$$r_{q_U} = \frac{|Infor(R_{q_U}) - \frac{\sum_{i=1}^{n} Infor(R_i^g)}{n}|}{\frac{\sum_{i=1}^{n} Infor(R_i^g)}{n}}, \tag{9}$$

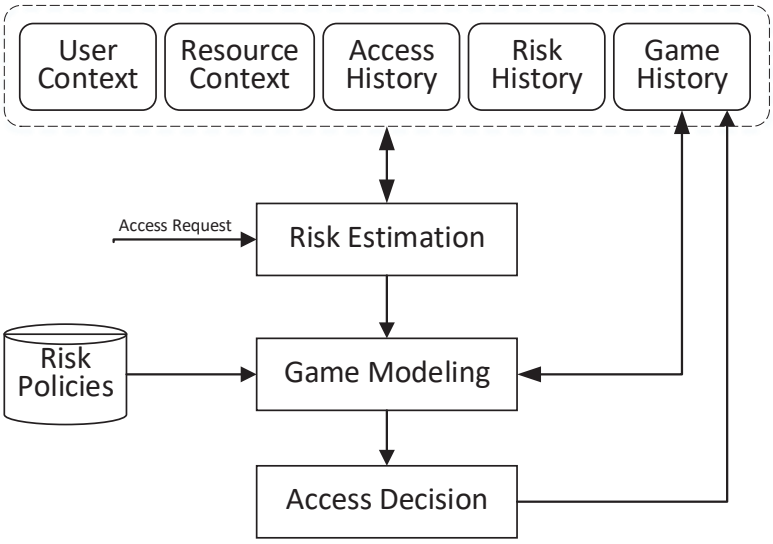

图 7: 基于博弈论风险适应性访问控制框架(RaBAC)

将用户的风险r_U^i计算为

$$r_U^i = \begin{cases} r_U^{i-1}(1-\dfrac{\alpha}{r_{max}}), & 若q_U是正常访问请求; \\ r_U^{i-1}(1+\dfrac{\beta}{r_{max}})), & 反之。 \end{cases} \tag{10}$$

将基于风险适应性的访问控制建模为一种隐私保护的博弈模型，其中涉及参与者、参与者策略和参与者效用函数。在这个博弈中，有两个参与者，服务提供者 S 和用户 U 。服务提供商拥有隐私敏感的资源（即访问客体），并希望授权正常访问请求并拒绝侵犯隐私的访问请求；用户是访问主体，其因为经济或其他利益而希望尽可能多地访问这些访问客体。用户 U 有两种策略，执行正常访问 N 和执行违反隐私的访问 V ；服务提供商 S 有两种策略，分别授权正常请求 G 和拒绝正常请求 D 。该博弈模型是一个多次博弈过程，可以分别考虑每次博弈的策略选择关系，并将每个子博弈视为一个独立博弈。假设此博弈中有 T 次子博弈，且 $\sigma_1^*, \sigma_2^*, \cdots, \sigma_T^*$ 是独立阶段博弈的Nash均衡策略的有序序列，然后该序列存在子博弈完美均衡，且均衡路径由 $\sigma_1^*, \sigma_2^*, \cdots, \sigma_T^*$ 生成。在每个阶段的博弈中都会求得最佳策略选择解。服务提供商和用户都可以获得最大的收益，且单次子博弈都可以达到Nash均衡。因此，用户将执行正常访问，而服务提供商将准许用户的正常访问请求。因此，服务提供商通过限制隐私侵害访问来保护信息资源中涉及的隐私信息。

6. 基于演化博弈的理性隐私风险访问控制模型

社交网络、医疗信息系统等以数据为中心的大规模用户(访问者)开放信息系统，亟需能够保护隐私的细粒度自适应访问控制模型，且需实现数据隐私保护需求和数据效用需求的平衡。现有基于理性的访问控制模型难以满足适应性保护隐私的需求，且博弈参与者的完全理性假设太强，不符合实际场景。基于风险访问控制能够实现细粒度的访问控制隐私保护目标，但如何进一步放松参与者完全理性的假设，并实现隐私保护与数据效用关系的动态平衡，仍需要进一步研究。

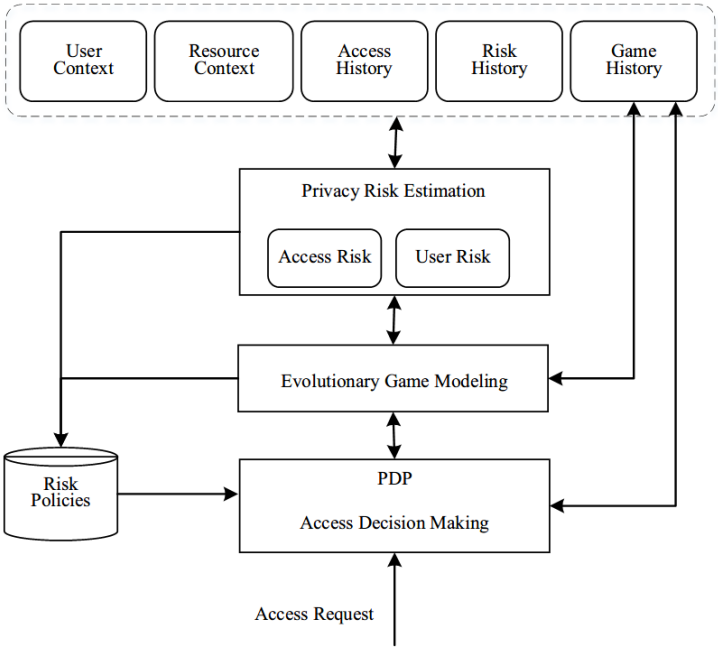

图 8: 基于演化博弈的隐私风险访问控制模型

针对这些问题和需求，在提出的风险自适应访问控制模型和完全理性隐私风险访问控制模型的基础上，进一步提出一种面向隐私保护的有限理性风险自适应访问控制模型，如图8所示。新提出的模型包含了新的隐私风险量化模块和演化博隐私弈决策模块。该模型首先基于信息量对访问请求的数据集隐私信息量进行量化，构造了访问请求隐私风险函数和用户隐私风险函数；其次，基于演化博弈在有限理性假设下构建多参与者的访问控制演化博弈模型，利用复制动态方程分析了访问控制参与者的动态策略选择和演化稳定状态形成机理，提出了隐私风险访问控制博弈演化稳定策略的选取方法。仿真实验和对比表明，所提出的访问控制模型能够有效动态自适应地保护敏感信息资源系统中的隐私信息，具有更好的隐私风险适应性，有限理性参与者的动态演化访问策略选取更加符合实际场景。

在该模型中，用户 U 的当前访问请求 q_0^U 隐私风险为

$$r(q_0^U)=\begin{cases}1, & 若R_0^U/R^g\neq\varnothing\\ \alpha\frac{-|R_0^U/R^U|max_{x\in R_0^U/R^U}logp(x)}{-\sum_{x\in R^U}logp(x)}+\beta\frac{-\sum_{x\in R_0^U\cap R^U}logp(x)}{-\sum_{x\in R^U}logp(x)} & 若R_0^U/R^g=\varnothing\end{cases} \tag{11}$$

当前访问请求 q_0^U 发出之后，系统根据其隐私风险值 r_n^U 和访问请求 q_0^U 的隐私风险值 $r(q_0^U)$ 计算用户 U 的更新隐私风险值

$$r_{n+1}^U=\begin{cases}r_n^U+r(q_0^U), & 若q_0^U是一个隐私侵犯访问请求;\\ r_n^U-r(q_0^U), & 反之。\end{cases} \tag{12}$$

在此基础上，构建了基于风险访问控制的演化博弈模型，即，风险自适应访问控制演化博弈模型，可表示为4元组 $raBACEGM=(P,A,\Pr,u)$ 。

1. $p=\{U,S\}$ 是演化博弈的参与者空间，其中 U 是用户， s 是信息资源系统。

2. $a=\{A_U,A_S\}$ 是博弈策略空间，其中 $A_U=\ \{Normal,Malicious\}$ 是用户的可选策略集合，包含正常访问和恶意访问两种， $A_S=\{Grant,Deny\}$ 是信息资源系统的可选策略集合，包含授权和拒绝两种。

3. $\Pr=\{p,q\}$ 是博弈信念集合，其中 $p=\{p_{Normal},p_{Malicious}\}$ 表示用户分别采取正常访问和恶意访问的概率，且 $p_{Normal}+p_{Malicious}=1$ ； $q=\{q_{Grant},\ q_{Deny}\}$ 表示信息资源系统分别采取授权和拒绝的概率，且 $q_{Grant}+q_{Deny}=1$ 。

4. $u=\{u_U,u_S\}$ 是博弈参与者的收益函数集合，其中 $u_U=\{u_U^{N,G},u_U^{N,D},u_U^{M,G},u_U^{M,D}\}$ 是用户的收益函数， $u_S=\{u_S^{N,G},u_S^{N,D},u_S^{M,G},u_S^{M,D}\}$ 是信息资源系统的收益函数，二者的值由参与者的访问策略选择所决定。

给定不同的策略选取初始状态，经过演化，所提出的风险自适应访问控制模型在演化博弈过程中会达到某个稳定状态。通过对比，本演化博弈模型的模拟演化结果与理论分析保持一致，说明该演化博弈模型与现实系统中的规律相符。所提出的风险自适应访问控制演化博弈模型具有有效性，可将其应用于面向隐私保护的风险自适应访问控制系统中，为访问控制系统的参与者进行隐私保护访问策略选取提供依据。

关键词： 隐私度量，隐私推断分析，理性隐私保护，信息论，博弈论

Rational Privacy Preserving Model and Its Application

Summary

Great challenges of data security and privacy are arising along with data growing massively, computing clouding, and application complicating. It is especially important to understand privacy and implement dynamic privacy preserving. And there is still a huge challenge in achieving balance between privacy protection and data utility. The non-cryptographic-based privacy research fields mainly include three aspects, i.e. privacy definition and quantification, privacy analysis and inference, and privacy preserving mechanism. The solution of these issues can help the community to improve its basic theoretical foundation, and provide solid specificity for privacy definition and measurement, privacy breach mechanism and privacy preserving, and then provide a route to balance privacy protection and data utility.

To address the mentioned critical scientific challenges, this work focuses on data opening and sharing scenarios, and non-cryptographic privacy domain. We mainly conduct research on privacy quantification, privacy analysis attack, privacy preserving, and the balance between privacy protection and data utility by using information theory and game theory. Several specific advances aiming to achieve rational privacy preserving and its application are suggested. After proposing a unified privacy quantification model based on information communication model, attribute privacy inference attack models on independent sequence data and related sequence data are suggested respectively, and the breached privacy and strength of adversaries are quantified by our proposed privacy quantification model. Further, a risk adaptive based access control(RaBAC) model for dynamic privacy preserving is proposed, And additionally, two rational privacy RaBAC models are proposed by using extensive game and evolutionary game, respectively. During the rational privacy RaBAC models, functions for estimating privacy risk value of access request and utility of data are suggested, and thus the balance between privacy protection and accessed data utility is achiein data opening and sharing scenario. More specific contributions of this thesis are as follows.

1. A unified privacy communication model for measuring privacy definition and quantity, strength of privacy analysis attack, and strength of privacy preserving mechanism, is proposed by using Shannon information. Several privacy quantification models of scenarios such as privacy preserving with/without adversary, privacy preserving with

multi-privacy resources, are suggested for the measuring requirements of privacy definition, privacy analysis attack and privacy preserving mechanism. Furthermore, methods for quantifying the strength of privacy analysis attack and privacy preserving mechanism are proposed, and these methods provide support to measure the quantity of privacy disclosure, the strength of privacy analysis attack and privacy preserving mechanism.

2. A privacy analysis attack model based on probability inference is proposed for the privacy of independent genetic data attributes in sequential data sharing scenarios. The model analyzes the interrelationship between the individual gene sequence attribute values and constructs the adversary model of the target attribute value inference. Based on the proposed adversary model, genome sequence privacy analysis attack methods are proposed based on an improved hidden Markov model and regression convolutional neural network model, respectively. Based on the privacy quantification model, attribute privacy and quantification methods of sequence data are defined, and these definitions are applied to quantify attribute privacy leaks and adversary acquisition. Experiments show that the proposed method is better than the existing genome sequence attribute privacy analysis model and algorithm. The error rate and uncertainty of the attribute privacy of the adversary are reduced, and the amount of private information obtained by the adversary is more than the existing work.

3. An attribute privacy probability inference model is constructed for family members' associated gene sequence data sharing scenarios. This model constructs an attribute privacy adversary model based on family pedigree structure and belief propagation model. Based on the defined sequence data attribute privacy quantification method, we analyze the impact of individual's sequence attribute privacy breached by using his family members sharing part of the private gene data. Experiments and comparisons show that family members sharing personal genome privacy data can seriously reveal the privacy of other family members. By publishing genetic data on the Internet and shared genetic data by family members, the gene attribute privacy of other family members can be attacked on a large scale. The proposed method is better than the results of the existing work, and the accuracy of the inferred attribute privacy is higher, the adversary has less uncertainty about genome attribute privacy, and acquires more genome privacy information.

4. Aiming at the dynamic privacy protection requirements of data sharing applications, a risk adaptive based access control model for privacy preserving is proposed based on XACML. After proposing the privacy preserving access control adversary model, three components, namely risk estimation, session control and risk mitigation services are added to the standard XACML framework, and other components are enhanced. In the new components, definition and quantification method of access request risk are proposed by using Shannon information entropy. The access request type discriminating method is proposed by combing access control request risk and the user's own risk. By using quantification of access request risk and credit card incentives, the system dynamically and adaptively constrain user access behaviors. The comparison and analysis show that the proposed model and method are more dynamic than the existing work, and achieve privacy protection and better usability.

5. A extensive game based rational privacy RaBAC model is proposed by employing Shannon information and game theory. After defining the concept of privacy risk and privacy violation access, this thesis proposes a framework and workflow for privacy risk access control model based on game theory. Calculation methods of access request's privacy risk and the user's privacy risk are propsed by using Shannon information. The conflict and cooperation relationship between the user and data service provider in the RaBAC of privacy protection is proposed by multi-stage two-player game. The analysis shows that there is a sub-game refining Nash equilibrium in stage game of the privacy RaBAC, which can balance the privacy protection and access data utility by limiting the privacy violation access request. This method benefits more than the existing work. It has the advantage of requiring less auxiliary information and providing more risk adaptability and privacy preserving.

6. A evolutionary game based rational RaBAC model for privacy preserving is proposed. The model includes a new privacy risk estimation module and an evolutionary game module. Firstly, based on the amount of information, the privacy information of the data set of the access request is quantified, and the access request privacy risk function and the user privacy risk function are constructed. Secondly, the multi-participant access control evolutionary game model is constructed under the assumption of bounded rationality by

using evolutionary game theory. The dynamic mechanism selection and evolution stable state formation mechanism in the game process are analyzed by the replication dynamic equation. The selection method of game evolution stability strategy is proposed. Simulation experiments and comparisons show that the proposed access control model can effectively and adaptively preserving private information, and has better privacy risk adaptability. The dynamic evolution of access policy selection of bounded rational participants is more in line with the actual scenario.

Keywords: Privacy quantification, Privacy inference attack, Rational privacy preserving, Information theory, Game Theory