# 通过参加“PWS Cup 攻防赛”以提升学生科研能力之探索*

马瑞强 [1,2,3**] 崔旭 [1] 郭亚楠 [1] 杨皓然 [1]

1 内蒙古工业大学网络空间安全学院，呼和浩特 010051
2 明治大学研究知财战略机构，日本东京 164-8525
3 内蒙古自治区北疆网络空间安全重点实验室，呼和浩特 010080

**摘 要** 随着信息技术的飞速发展，信息安全问题已成为全球关注的焦点。信息安全人才的培养需求日益迫切。信息安全攻防竞赛作为一种极具实践性的教育模式，不仅能够增强学生的技术能力，还能够通过实战训练促进学生的科研创新能力。本论文旨在探讨通过日本信息安全攻防竞赛（PWS Cup & iPWS Cup）以促进学生在数据安全算法与评价领域的科研能力增长，并且期待将以此为教学引导模式，渗入研究生的培养工作。通过连续两年四次参加此项比赛，从成绩排序到知识积累均取得了较大的进步，为我校网络空间安全研究生实战能力培养，迈出了新的步伐和提供了新的思路。

**关键字** 信息安全，攻防竞赛，差分隐私，k-匿名，科研能力育成

# Exploring the enhancement of students' research ability by participating in the “PWS Cup Offense and Defense Competition”

Ruiqiang Ma [1,2,3*] Xu Cui [1] Yanan Guo [1] Haoran Yang [1]

[1]College of Cyber Security Inner Mongolia University of Technology, Hohhot 010051, China
[2]Reasearch on Financial Strategic Institutions Meiji University, Tokyo 164-8525, Japan
[3]Inner Mongolia Key Laboratory of Beijiang Cyberspace Security, Hohhot 010080, China

**Abstract—With the rapid development of information technology, the issue of information security has become a global concern. The demand for the training of information security talents is becoming more and more urgent. As a very practical educational mode, information security attack and defense competitions can not only enhance students' technical ability, but also promote their scientific research and innovation ability through practical training. In this thesis, we aim to promote students' research ability in the field of data security algorithms and evaluation through the Japan Information Security Cup (PWS Cup & iPWS Cup), and we expect that this will be used as a model for teaching and learning, which will permeate into the training of graduate students. By participating in this competition for four times in two consecutive years, we have made great progress from the ranking of results to the accumulation of knowledge, and have taken new steps and provided new ideas for the cultivation of the practical ability of graduate students in cyberspace security in our university.**

**Keywords—Information Security, Attack and Defense Competitions, Differential Privacy, K-anonymity, Research Capacity Breeding**

## 1 引 言

在大数据时代，信息安全的重要性不断提升。然而，当前许多高校的信息安全教学主要以理论为主，实践环节较为薄弱，导致学生的动手能力和创新思维一定程度上受到限制。如何将实践与理论更好的结合，培养具备科研能力和实战经验的工业信息安全人才，成为高校网络空间安全专业教学改革中的重要课题。信息安全攻防竞赛作为一种实践性极强的实战竞赛模式，在一定程度上能够弥补这一不足。本文将探讨如何通过参加日本 PWS Cup 攻防赛提升研究生的科研能力，提出相应的教学改革方案。

基于我大学的研究生创新能力提升专项行动，开展专业学位研究生的实践创新训练模式研究。针对本研专业型硕士研究生的社会需求实际，进行差异化、理论化与实训化相结合的培养，完善协同育人机制、专业学位人才培养模式、锻炼专业学位研究生

*基金资助：本文得到内蒙古工业大学研究生院以赛促研教改(RC2300003890）和专创融合课程建设(ZC2024045)资助。
**通讯作者： 马瑞强 marq@imut.edu.cn

导师队伍建设。本学拥有研究内容为信息安全方向的课题，具有较强的实践应用性，是理论与实践同等重要的一门学科。通过主动参与国际优秀平台的公开数据安全攻防赛活动，需求导向驱使学生有针对性地去解决工业生产的实际问题，而且实时在线评估本方参赛算法的有用性与安全性，诸如此类的评判算法几乎是未曾接触过的。同时平台会促使师生去分析来自各方的优良提案与算法，为我所用改进本方策略的同时拓展检索全球相关研究的最新成果。目标明确、探求欲强、解决问题迫切，学、用、研紧密结合，个人技能全方位提升。同时期待形成一套实用完善的以赛促研的新型教改体系。

# 2 相关工作

## 2.1 当前信息安全教学的不足

（1） 理论与实践存在脱节

目前，许多高校的信息安全课程仍以理论授课为主，学生缺乏足够的实践机会。在传统教学模式下，学生虽然掌握了密码学、网络协议分析、恶意软件分析等基础知识，但在实际操作中常常难以应对复杂的网络安全问题。理论学习与实践脱节导致学生缺乏解决实际问题的能力。

（2）科研创新训练不足

研究生阶段的学习不仅仅是技能的培养，更强调创新能力的提升。然而，传统的信息安全教学鲜有涉及创新训练，学生难以通过自主研究和实践结合而产生新的科研成果。

（3） 实际应用场景有限

信息安全是一个高度实践导向的学科领域，真实的网络攻击环境非常复杂。在课堂教学中，学生缺乏真实的应用场景，对数据以及数据间关联性理解存在感性认识，难以在复杂环境中锻炼信息安全防护能力。

# 3 信息安全攻防竞赛概述

## 3.1 传统的 CTF 竞赛

CTF（Capture The Flag）是一种模拟真实网络环境的安全竞赛，参赛者通过破解系统、分析漏洞、设计攻击或防御策略等方式完成任务。CTF 竞赛包括破解题、逆向工程、漏洞利用、密码学、网络取证等多种题目类型，提交以演算、专题解答等为主，要求参赛者具备深厚的技术知识和强大的问题解决能力。

CTF 竞赛不仅考验学生的技术能力，还强调思维创新、团队协作、时间管理等多种软技能。通过参与 CTF 竞赛，学生可以在实际操作中提升自己的技能水平，并积累宝贵的科研经验。

## 3.2 关于 PWS Cup

PWS Cup 是日本最具权威的信息安全攻防竞赛模式，日本高校、企业、政府的法律部门等均深度参赛。随着国内外大数据利用需求的快速增长，网络安全和信息安全的重要性日益增强，迫切需要开发和建立平衡数据有效利用和隐私保护的技术和标准。为此，日本信息处理学会计算机安全研究组（CSEC 研究组）在 2015 年第一次成立了 PWS 组委会，并与该会安全心理与信任研究组（SPT）联合主办了“隐私研讨会（PWS）”研究小组。 PWS 每年与计算机安全研讨会（CSS）同期举办，主要由围绕隐私保护技术促进数据利用的项目和会议组成。

为了加快国际化进程的步伐，从 2023 年始推出了国际版 iPWS Cup，iPWS Cup 是一项国际数据匿名化赛事，报名不收取任何费用，它是日本国内同类 PWS Cup 首次面向国际学者及感兴趣群体。iPWS Cup 要求每个团队同时承担匿名者和攻击者的双重身份，旨在确定有效的匿名化方法，并通过让每个团队参与实际的匿名化和随后的攻击模拟来培养专业知识。iPWS Cup 鼓励参与者在保护数据隐私和保留数据效用之间取得平衡。

# 4 教学改革设计方案

为了有效提升研究生的科研能力，本研究提出了一套结合信息安全攻防竞赛的教学改革方案。该方案将 CTF 竞赛融入信息安全教学的各个环节，通过项目式学习、竞赛驱动、跨学科合作等方式全面提升学生的综合能力。

① 从我院实际出发，坚持理论研究和教改实践相结合的原则，在充分论证的基础上，在相关学科的硕士生范围内展开；

② 在具备信息安全基础知识及 Python/C/Ruby 等其中之一的编程能力的前提下，研读与消化过往优秀平台所使用的策略、评价机制、样例代码；

③ 研究与理解原始数据的来源及组合理论与方法，调研此类策略的原始论文来源并再现之。信息安全，数据是核心也是载体，数据的优劣将决定平台的质量，深入了解其行业评价方法；

④ 理论与实践相结合是专业型研究生教育教学研究中的重点和难点，以赛促研非常值得一试。而且平台中不乏世界著名学府或政府背书下的信息产业研究院，其攻防算法多采用传统与新型相结合的模式，优中选优，为我所用；

⑤ 平台通过分为预备与决赛两个阶段，权重各有差异、算法规定也不尽相同、评价指标渐趋苛刻，此时，要在理论基础上，灵活采用擅长的编程语言实现算法。对于这样分段式成果模式的赛事，学生们中可各显其能，不限于某一种语言编程，比较灵活地实现本方算法，且分段提交以校验本方在全局中的排序，以更好地提出应对措施；

⑥ 举办总结汇报与表彰大会，各队讲解在历时三个月的各自团队的攻防策略与心得，成果以 Poster 形式展示，这对学生成文的锻炼非常有益，全员参与、择优处拼接，提出终版并形成英文答辩材料，参与后续演讲。通过交流、结合本队对数据脱敏以及被攻击的实际情况，体会对方算法的优劣，加深对安全算法在工程实践中应用的理解，印象深刻、永生难忘。

⑦ 整个过程的节点事件及成果，在本研 Web 中反应以共享，并链接优秀队成果、攻防过程、思维脉络、参考论文。最后，总结成果，以研究论文和可行报告方式形成最终教改成果。

为了有效提升研究生的科研能力，本研究提出了一套结合信息安全攻防竞赛的教学改革方案。该方案将 CTF 竞赛融入信息安全教学的各个环节，通过项目式学习、竞赛驱动、跨学科合作等方式全面提升学生的综合能力。

### 4.1 竞赛驱动教学模式

CTF 竞赛可以作为教学的补充和延伸，激发学生的兴趣并培养其科研思维。具体策略如下：

课程嵌入 CTF 竞赛：将 CTF 竞赛的题目直接引入课程教学中，作为课堂练习或课程项目。竞赛题目涵盖逆向工程、二进制漏洞、Web 安全、密码学等多学科内容，帮助学生加深对理论知识的理解。

学术竞赛结合科研：引导学生通过分析竞赛中的技术问题，发现科研课题。教师可以结合实际竞赛中的难点问题，指导学生进行深入研究，撰写科研论文。

### 4.2 跨学科合作

信息安全领域往往涉及多个学科，如计算机科学、数学、法律等。通过跨学科合作的方式，学生不仅可以提升技术能力，还能扩展视野，提升创新能力。具体实施措施如下：

信息整合：将信息安全课程与其他相关课程（如法律、社会学、数学）结合，帮助学生全面理解信息安全问题的多维度属性。

跨专业团队协作：鼓励学生与其他专业的同学合作，共同完成跨学科的科研项目。例如，法律专业的学生可以研究信息安全中的法律问题，而技术专业的学生则负责开发和实施技术方案。

### 4.3 教师培训与科研指导

特别带领对年轻教师技能提升：教师的能力对教学改革起到关键作用。通过定期组织教师参与信息安全培训和 CTF 竞赛，提升其实践能力和科研水平。

科研项目支持：为学生提供相关科研项目的支持，鼓励其参与国家或校内外的科研项目，将竞赛中的成果转化为科研成果。

### 4.4 PWS Cup 介绍及资源

由于在数据发布的同时需要确保个人隐私得到保护，然而攻击者试图通过利用公开数据泄露个人秘密，扰乱社会秩序。在这种情况下，每个团队同时扮演匿名者和攻击者的角色，在数据匿名化技术和对匿名数据的攻击方面进行竞争。在数据匿名化阶段，每个团队都扮演一家想要发布客户数据的公司的角色，旨在通过对给定数据进行匿名化来保护数据中人员的隐私。在攻击阶段，每个团队都成为一个想要发现数据内容的攻击者，目的是发现其他团队匿名化的数据中包含的关于个人的更多秘密信息。

## 5 竞赛实践的预期效果

### 5.1 技术能力提升

通过 PWS 竞赛的驱动，学生能够在实践中快速提升技术能力，掌握漏洞分析、系统攻击与防御、数据分析等核心技术。同时，通过项目式学习的训练，学生能够在复杂环境中应对多种安全挑战。

### 5.2 科研能力增强

通过竞赛驱动和跨学科合作，学生在参与竞赛的过程中，能够逐步发现学术问题，锻炼科研思维。这一过程中，学生不仅积累了丰富的技术经验，还能将竞赛中的问题转化为科研课题，撰写学术论文或进行技术创新。

### 5.3 创新能力培养

信息安全领域技术变化迅速，竞赛题目往往需要参赛者在短时间内找到创新性解决方案。通过竞赛驱动的教学模式，学生能够不断锻炼其创新思维，培养在科研工作中发现问题和提出创新性解决方案的能力。

## 5.4 学术与实战相结合

竞赛与科研的结合，使学生能够在实际操作中应用所学理论知识，并通过科研项目的深入探索，进一步巩固和提升其理论水平。这种理论与实践相结合的学习模式，能有效提高学生的综合素质和就业竞争力。

## 5.5 攻防赛详细

（1）背景介绍

在 iPWS Cup 2023 的竞赛中，为研究人员提供包含诊断结果的健康数据，以预测患糖尿病的风险。这些数据包含的记录包括极高的身体质量指数(BMI)。在匿名化阶段，iPWS 杯 2023 的每个参赛队都将匿名化健康数据，以防止识别体检者。在攻击阶段，每支队伍会检查其他队伍生成的匿名数据是否包含本队的记录。一旦检测到包含，就从匿名数据中识别出记录。

在 iPWS Cup 2024 的竞赛中，公司 A 想要开发一个使用客户数据的电影推荐系统。该公司决定将客户数据匿名化，用于开发推荐系统的竞赛，并将其提供给竞赛的参与者。然而，即使有意将数据匿名化，由于与外部数据匹配，也出现了个人身份识别和隐私泄露的情况。但是“数据库重构攻击”的问题导致匿名化的数据并不安全，即使是匿名后的数据，也可以与本应安全的统计数据相结合，重构原始数据。

（2）竞赛规则介绍

目前，国际版赛事已举办两次，两次赛事使用的数据集不同，2023 年使用的是 NHANES[16] 2017-2018(National Health and Nutrition Examination Survey)多个数据表整合数据，而 2024 年使用的是由 MovieLens 生成的虚拟数据。两次竞赛在规则上稍有差异，但是整体流程基本一致。如图 1 所示，数据攻防赛由两个阶段组成：匿名阶段和攻击阶段，如下所述。

匿名阶段：保护自己团队数据，以减少他组对本组匿名数据的识别。

① 每个团队接收多份不同的数据 $B^i$，选取其中一个作为本队匿名的原始数据。

② 各队对原始数据 $B^i$ 匿名化，使用本队方法生成匿名数据集 $C^i$ 并提交给组委会。

③ 根据提交的 $B^i$ 和 $C^i$ 评估数据的有用性。

攻击阶段：识别其他队伍数据，尽可能更多的地识别他组样本记录。

① 组委会将各队提交 $C^i$ 提取部分样本 $D^i$ 以及对应索引 $X^i$，将各队数据 $B^i$ 及 $D^i$ 分发给参赛队伍。

② 各队使用攻击方法来识别 $D^i$ 中数据对应 $B^i$ 中行索引，并提交索引结果 $E^i$。

③ 组委会比较 $D^i$ 和 $E^i$，计算 $D^i$ 中未被识别行的比例来评估隐私分数。

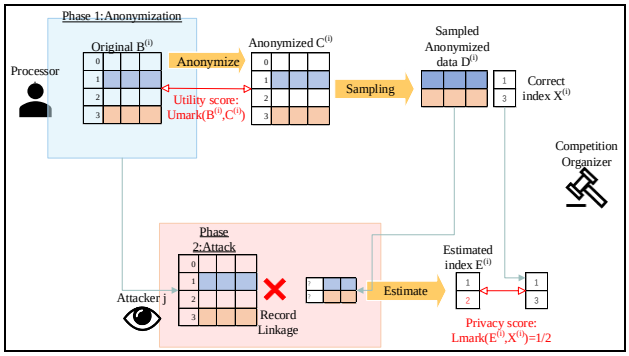


图 1 iPWScup2024 数据匿名竞赛规则

（3）竞赛评分标准

**效用分数(U)**：匿名化后数据的效用保留多少。评分从 1（最好）到 0（最差），其中 1 表示匿名化的数据与原始数据具有完全的效用（无损失）。如下公式(1)：

$$U(T^*)=\sqrt[6]{\prod_{i=1}^{6}(1-P_i)} \tag{1}$$

计算匿名数据集的有用性时，需要考虑多个因素 Pi，其中包括数值型(Age、BMI)与分类型数据(Cat)的最大信息损失、最大患病比例(Rate)、最大比值比(OR)以及最大相关性系数(Cor)。

**隐私分数(P)**：数据的隐私在多大程度上受到了保护，不受其他团队的攻击。得分范围从 1（最好）到 0（最差），其中 1 表示样本匿名数据中的任何记录都没有被任何团队识别，0 表示至少有一支团队全部识别了本队样本匿名数据的所有记录。如下公式(2)：

$$P=\frac{N_{un}}{N_{sample}} \tag{2}$$

其中 $N_{un}$ 表示样本数据中未被识别的数据数量，$N_{sample}$ 表示样本数据总数量。选取其他队伍对本队攻击效果最佳(即最低隐私性得分)作为本队的隐私性得分。

匿名健康数据的最终得分是其效用得分与隐私得分的调和平均值。如下公式(3)：

$$Score=\frac{2}{(U^{-1}+P^{-1})} \tag{3}$$

IL($N_i$)表示数值型数据的信息损失，如下式所示(4)：

$$IL(N_i)=\frac{|T(N_i)-T^*(N_i)|}{20} \tag{4}$$

其中，i 表示数据集中属于连数值型数据的列索引，$T(N_i)$和 $T^*(N_i)$分别表示原始数据集与匿名数据集中数值型数据的取值。

IL($C_j$)表示分类型数据的信息损失，如下式所示(5)：

$$IL(C_j)=\begin{cases}\dfrac{1}{Num(C)} & T(C_j)!=T^*(C_j)\\ 0 & T(C_j)=T^*(C_j)\end{cases} \tag{5}$$

其中，j 表示数据集中属于分类型数据的列索引，$T(C_j)$和 $T^*(C_j)$分别表示原始数据集与匿名数据集中分类型数据的取值，Num(C)具体表示为数据集中更改过的数据属性个数。

IL(t)表示元组的信息损失，如下式所示(6)：

$$IL(t)=\sum_{i=1}^{n}IL(N_i)+\sum_{j=1}^{m}IL(C_j) \tag{6}$$

其中 n、m 分别表示数值型数据与分类型数据个数。因此，数据集的平均信息损失如下式所示(7)：

$$IL(T)=\frac{\sum_{i=1}^{N}IL(t_i)}{N} \tag{7}$$

（4）以赛促研成效与反馈

学科竞赛不仅能够检验学生的学习效果，也能够检验高校人才培养的质量和效果。以赛代练、赛练结合，是个能够提高学生实践能力的好方法。以赛促研是一种有效的教育教学方法，通过比赛促进教师与学生的钻研和创新能力，从而提高教学质量和研究成果。这种方法不仅激发了教师的积极性，还提升了教师的教学和研究能力，形成了良好的教学和研究氛围。具体而言，以赛促研的成效主要体现在以下几个方面：首先，比赛促进了教师和教学人员的钻研能力，深入挖掘研究内容，提升了教学质量。其次，比赛激发了教师的创新意识和能力，促使学生在研究中融入新的理念和方法。最后，竞赛还促进了各国研究人员之间的交流与合作，形成良好的团队合作氛围。

总之，以赛促研不仅提高了教师的教学和研究能力，还促进了教学质量的提升和研究成果的产出，形成了良性循环的教学与研究环境。

此次竞赛采用攻防对抗的形式，参赛队伍需要模拟真实的数据应用环境，分别作为攻击方与匿名者，在规定时间内完成攻击与匿名。数据隐私保护攻防赛涉及计算机科学、密码学、数据科学等多个学科领域。参赛者需要综合运用各学科知识，形成跨学科的解决方案。通过参加此类竞赛，参赛者能够接触到最新的技术动态和研究成果，从而激发创新思维，推动技术创新。竞赛对于培养具有创新精神和实践能力的高素质人才具有重要意义。参与竞赛的学生能够获得宝贵的实践经验，提升解决实际问题的能力，为未来的职业发展打下坚实基础。数据隐私保护是全球性的问题，来自不同国家和地区的同行共同探讨解决方案，强化国际合作与交流。

随着数据隐私保护问题的日益突出，竞赛所体现的社会影响力也在不断提升。通过竞赛的举办和宣传，更多的人开始关注数据隐私保护问题，提高了社会的整体安全意识。竞赛中的许多创新技术和解决方案在进一步优化后，成功应用于医疗、金融、电商等行业的数据隐私保护。这些应用不仅提高了数据的安全性，还促进了业务的合规性和效率。竞赛的举办和宣传不仅增强了专业人士对数据隐私保护的重视程度，还通过媒体和网络向公众普及了数据隐私保护的重要性，这种教育作用有助于提升全社会的数据安全意识。竞赛中的优秀技术和算法经过产业界的验证与优化后，能够更好地满足市场需求，推动产业与科研的深度融合。这种融合有助于形成产学研用一体化的良性循环，促进数据隐私保护领域的持续发展。

此次竞赛中，PWS Cup 分为预赛和决赛两个阶段，且每个阶段根据匿名分数与攻击分数分别计算成绩，综合成绩按预赛成绩 10%，决赛成绩 90%来求和。图 2 为此次 PWS Cup 竞赛的综合成绩表。该图中我组为第 4 组，对应行位其他组攻击我组的分数，而对应列为我组攻击其他组的得分，下图中 anonymity 为匿名分数，即 100 减其他组攻击我组的最高得分 34，utility 为我组匿名后的数据有用性分数，total 则为该阶段的最终得分，即 anonymity 与 utility 之和，此为决赛阶段总分数。图中 pre total 为预赛阶段总分数，pre total 与 total 按照 1:9 的比例计算出综合成绩（overall score），图中最后一列 overall rank 对应每组的综合排名。此次 iPWS Cup 同样分为匿名与攻击两部分，然而与 PWS Cup 的不同之处在于，iPWS Cup 无预赛决赛之分，计算匿名分数与攻击分数即可得最终结果。图 3 为此次 iPWS Cup 竞赛的最终成绩。

本组为第一组，可以看出在竞赛中的表现具有一定的亮点，但也存在一些可以进一步优化的空间。总体来看，本组在匿名性、效用性和平衡隐私保护与数据可用性之间表现出较为均衡的能力，但在面对高强度攻击时的防御能力尚有提升空间。

| | | attacker | | | | | | | | | | | | | | | | | | | | | main | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | sample | anonymity | utility | total | total rank | pre total | overall score | overall rank |
| anonymizer | 01 | 0 | 28 | 14 | 14 | 13 | 17 | 20 | 0 | 19 | 23 | 26 | 18 | 0 | 17 | 22 | 68 | 14 | 18 | 5 | 69 | 27 | 0 | 88 | 31 | 91.02 | 84.02 | 13 | 146.5 | 90.268 | 12 |
| | 02 | 33 | 0 | 13 | 12 | 13 | 15 | 16 | 0 | 14 | 16 | 21 | 22 | 0 | 14 | 11 | 51 | 15 | 15 | 10 | 55 | 16 | 0 | 87 | 45 | 83.69 | 118.69 | 10 | 147.61 | 121.582 | 9 |
| | 03 | 40 | 38 | 0 | 25 | 32 | 34 | 21 | 0 | 26 | 25 | 35 | 30 | 0 | 17 | 32 | 58 | 36 | 29 | 6 | 69 | 38 | 0 | 84 | 31 | 76.76 | 69.76 | 17 | 124.38 | 75.222 | 16 |
| | 04 | 25 | 23 | 22 | 0 | 25 | 20 | 17 | 0 | 21 | 16 | 27 | 27 | 0 | 17 | 13 | 34 | 33 | 19 | 8 | 29 | 17 | 0 | 81 | 66 | 69.1 | 135.1 | 3 | 135.38 | 135.128 | 1 |
| | 05 | 47 | 33 | 20 | 22 | 0 | 46 | 24 | 0 | 31 | 57 | 40 | 35 | 0 | 11 | 32 | 43 | 53 | 47 | 8 | 62 | 53 | 0 | 87 | 38 | 72.36 | 86.36 | 12 | 0 | 77.724 | 15 |
| | 06 | 68 | 34 | 21 | 16 | 24 | 0 | 20 | 0 | 17 | 32 | 55 | 29 | 0 | 18 | 20 | 41 | 81 | 26 | 8 | 55 | 14 | 0 | 85 | 19 | 74.55 | 31.55 | 18 | 20.45 | 30.44 | 18 |
| | 07 | 18 | 22 | 17 | 22 | 25 | 20 | 0 | 0 | 19 | 25 | 26 | 25 | 0 | 38 | 18 | 39 | 27 | 17 | 16 | 39 | 26 | 0 | 68 | 61 | 72.4 | 133.4 | 5 | 24.31 | 122.491 | 8 |
| | 08 | 49 | 23 | 19 | 14 | 41 | 47 | 19 | 0 | 22 | 45 | 54 | 43 | 0 | 13 | 22 | 31 | 60 | 0 | 5 | 35 | 39 | 0 | 84 | 40 | 63.3 | 83.3 | 14 | 0 | 74.97 | 17 |
| | 09 | 24 | 26 | 16 | 15 | 19 | 15 | 20 | 0 | 0 | 19 | 18 | 16 | 0 | 10 | 16 | 28 | 14 | 12 | 10 | 28 | 13 | 0 | 91 | 72 | 72.2 | 144.2 | 1 | 0 | 129.78 | 5 |
| | 10 | 29 | 33 | 21 | 19 | 14 | 12 | 14 | 0 | 24 | 0 | 23 | 16 | 0 | 11 | 13 | 43 | 16 | 14 | 6 | 51 | 20 | 0 | 92 | 49 | 86.1 | 133.1 | 6 | 132.31 | 133.021 | 3 |
| | 11 | 41 | 22 | 15 | 17 | 24 | 26 | 16 | 0 | 21 | 18 | 0 | 28 | 0 | 11 | 30 | 43 | 33 | 19 | 6 | 45 | 29 | 0 | 89 | 55 | 76.89 | 131.89 | 8 | 137.61 | 132.462 | 4 |
| | 12 | 40 | 33 | 22 | 17 | 16 | 24 | 25 | 0 | 25 | 29 | 32 | 0 | 0 | 16 | 19 | 51 | 30 | 25 | 7 | 68 | 27 | 0 | 86 | 32 | 80.17 | 76.17 | 16 | 144.47 | 83 | 14 |
| | 13 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 22 |
| | 14 | 15 | 18 | 15 | 12 | 12 | 14 | 11 | 0 | 17 | 17 | 11 | 13 | 0 | 0 | 14 | 16 | 17 | 14 | 8 | 17 | 14 | 0 | 87 | 82 | 50.63 | 132.63 | 7 | 0 | 119.367 | 10 |
| | 15 | 68 | 19 | 16 | 56 | 84 | 86 | 24 | 0 | 64 | 82 | 58 | 89 | 0 | 14 | 0 | 88 | 87 | 72 | 5 | 70 | 88 | 0 | 90 | 11 | 70.27 | 3.27 | 21 | 138.14 | 16.757 | 20 |
| | 16 | 34 | 23 | 18 | 17 | 18 | 16 | 19 | 0 | 20 | 19 | 23 | 16 | 0 | 13 | 8 | 0 | 22 | 14 | 8 | 58 | 21 | 0 | 90 | 42 | 82.02 | 108.02 | 11 | 134.47 | 110.665 | 11 |
| | 17 | 25 | 22 | 15 | 16 | 13 | 17 | 18 | 0 | 22 | 17 | 25 | 12 | 0 | 13 | 15 | 34 | 0 | 20 | 11 | 36 | 22 | 0 | 84 | 64 | 67 | 131 | 9 | 114.51 | 129.351 | 6 |
| | 18 | 12 | 17 | 15 | 16 | 52 | 50 | 23 | 0 | 16 | 54 | 15 | 52 | 0 | 6 | 22 | 11 | 18 | 0 | 7 | 17 | 17 | 0 | 85 | 46 | 29.38 | 26.14 | 19 | 25.71 | 26.097 | 19 |
| | 19 | 83 | 19 | 21 | 69 | 50 | 69 | 26 | 0 | 68 | 49 | 58 | 83 | 0 | 87 | 35 | 83 | 69 | 0 | 0 | 54 | 73 | 0 | 21 | 13 | 69.56 | 8.56 | 20 | 0 | 7.704 | 21 |
| | 20 | 26 | 28 | 23 | 18 | 21 | 26 | 28 | 0 | 25 | 26 | 20 | 20 | 0 | 18 | 17 | 34 | 21 | 18 | 5 | 0 | 21 | 0 | 89 | 66 | 72.08 | 138.08 | 2 | 0 | 124.272 | 7 |
| | 21 | 26 | 38 | 14 | 13 | 10 | 11 | 13 | 0 | 16 | 16 | 16 | 11 | 0 | 14 | 13 | 33 | 20 | 11 | 3 | 34 | 0 | 0 | 87 | 62 | 72.01 | 134.01 | 4 | 142.98 | 134.907 | 2 |
| | 22 | 45 | 28 | 25 | 23 | 14 | 25 | 23 | 0 | 23 | 26 | 33 | 26 | 0 | 0 | 13 | 48 | 27 | 20 | 7 | 63 | 31 | 0 | 91 | 37 | 70.38 | 81.38 | 15 | 136.09 | 86.851 | 13 |
| attack sum | | 748 | 527 | 362 | 433 | 520 | 590 | 397 | 0 | 510 | 611 | 616 | 611 | 0 | 358 | 385 | 877 | 693 | 410 | 149 | 954 | 606 | 0 | | | | | | | | |
| attack top5 | | 119 | 137 | 92 | 102 | 100 | 92 | 117 | 0 | 109 | 102 | 107 | 99 | 0 | 97 | 77 | 168 | 115 | 77 | 42 | 164 | 115 | 0 | | | | | | | | |
| attack rank | | 4 | 3 | 15 | 10 | 12 | 15 | 5 | 20 | 8 | 10 | 9 | 13 | 20 | 14 | 17 | 1 | 6 | 17 | 19 | 2 | 6 | 20 | | | | | | | | |
| pre attack top5 | | 105 | 107 | 56 | 77 | 65 | 82 | 85 | 0 | 102 | 114 | 71 | 98 | 0 | 65 | 99 | 61 | 83 | 67 | 0 | 107 | 73 | 100 | | | | | | | | |
| total attack | | 118 | 134 | 88.4 | 99.5 | 96.5 | 91 | 114 | 0 | 108 | 103 | 103 | 98.9 | 0 | 93.8 | 79.2 | 157 | 112 | 76 | 37.8 | 158 | 111 | 10 | | | | | | | | |
| total attack rank | | 4 | 3 | 16 | 11 | 13 | 15 | 5 | 21 | 8 | 10 | 9 | 12 | 21 | 14 | 17 | 2 | 6 | 18 | 19 | 1 | 7 | 20 | | | | | | | | |

图 2 PWScup2024（国内赛）综合成绩

从攻击成功率的角度分析，本组对他组的总攻击成功次数为 323 次，在所有参赛组中表现属于中等水平。尤其是在攻击成功较高次数的攻击中，本组的成功攻击次数达到 128 次，这一数据较为显著，表明高强度攻击对他组的匿名方法造成了一定的威胁。

| | | attacker | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 10 | sample | anonymity | utility | total | total rank | |
| anonymizer | 01 | 0 | 21 | 9 | 50 | 11 | 22 | 22 | 16 | 0 | 30 | 90 | 50 | 71.14 | 121.14 | 5 | |
| | 02 | 27 | 0 | 10 | 72 | 14 | 22 | 45 | 14 | 0 | 63 | 88 | 28 | 67.35 | 51.35 | 7 | |
| | 03 | 43 | 72 | 0 | 73 | 18 | 32 | 36 | 25 | 0 | 73 | 82 | 27 | 80.55 | 61.55 | 6 | |
| | 04 | 19 | 12 | 14 | 0 | 10 | 17 | 18 | 19 | 0 | 10 | 89 | 81 | 76.25 | 157.25 | 1 | 総合1位 |
| | 05 | 18 | 21 | 10 | 11 | 0 | 15 | 21 | 17 | 0 | 17 | 79 | 79 | 70.19 | 149.19 | 2 | 総合2位 |
| | 06 | 94 | 86 | 94 | 89 | 94 | 0 | 94 | 24 | 0 | 91 | 6 | 6 | 65.73 | 0 | 9 | |
| | 07 | 23 | 15 | 11 | 23 | 25 | 19 | 0 | 22 | 0 | 22 | 78 | 75 | 60.56 | 135.56 | 4 | |
| | 08 | 64 | 87 | 10 | 91 | 14 | 61 | 43 | 0 | 0 | 90 | 86 | 9 | 77.16 | 4.16 | 8 | |
| | 09 | 17 | 8 | 14 | 15 | 14 | 17 | 18 | 14 | 0 | 15 | 88 | 82 | 4.56 | 0 | 9 | |
| | 10 | 18 | 28 | 18 | 26 | 11 | 15 | 21 | 20 | 0 | 0 | 91 | 72 | 65.42 | 137.42 | 3 | 総合3位 |
| attack sum | | 323 | 350 | 190 | 450 | 211 | 220 | 318 | 171 | 0 | 411 | | | | | | |
| attack top5 | | 128 | 97 | 62 | 129 | 78 | 88 | 107 | 94 | 0 | 107 | | | | | | |
| attack rank | | 2 | 5 | 9 | 1 | 8 | 7 | 3 | 6 | 10 | 3 | | | | | | |
| | | | | | 攻撃1位 | | | | | | | | | | | | |

图 3 iPWScup2024(国际赛)综合成绩

在匿名性与效用性方面，本组表现出了一定的平衡能力，其匿名性得分为 50，效用性得分为 71.14，均处于中等偏上的水平。这反映出本组在数据匿名化的过程中既注重隐私保护，又兼顾数据的实际可用性，展现了较为成熟的设计思路。尤其是效用性得分较高，表明匿名处理后的数据仍能有效地满足实际应用需求。然而，与排名靠前的组相比，匿名性得分略显不足，这可能是导致该组在总评分中未能更进一步的原因之一。

在综合总分面，本组以 121.14 分的成绩在所有参赛组中排名第 5。这个成绩说明了本组在整体设计上的稳健性和综合能力，但同时也揭示了其在某些细节上的短板。从数据来看，如果能在匿名性上进一步提升，同时针对高强度攻击设计更有效的防御机制，本组的综合排名有望得到显著提高。

综上所述，数据隐私保护攻防赛在推动技术创新、提升人才质量、加强国际合作、增强社会影响力、促进行业应用与标准化、政策与法规支持、公众教育与意识提升、科研与产业融合等方面都取得了显著成效。这些成效不仅为数据隐私保护领域的发展提供了有力支持，也为其他领域的创新和发展提供了有益的借鉴与启示。

属性识别技术的描述，并远程参加了总结表彰大会，盛况空前（图 6），组长用英文介绍了自己的攻防策略，同与会者进行了充分交流。参赛队中包括东京大学、大阪大学等名校，以及丰田、SoftBank 等跨国公司，同台技艺，学生的创新能力与实践水平提到了大幅提升，有效推动了学生科研能力，这将为研究课题的推进，提供新的思路。


图 4 Poster 发表


賞 状
PWS Cup 2024 総合優勝
チーム名:Hots
馬 瑞強 殿(内蒙古工業大学)
郭 家揚 殿(内蒙古工業大学)
崔 旭 殿(内蒙古工業大学)
楊 皓然 殿(内蒙古工業大学)
2024年10月24日
一般社団法人 情報処理学会
コンピュータセキュリティ研究会
PWS組織委員会 PWS2024
実行委員長 千田浩司

图 5 冠军队表彰

图 6 经验交流会现场（日本）

## 6 结束语

通过信息安全攻防竞赛与课程的结合，不仅能够提升研究生的技术水平，还能够在实际操作中培养其科研能力和创新思维。本文提出的教学改革方案，通过两年四度全程参加日本信息安全攻防比赛，每次的总时长达 6 个月，利用 CodaBench 等工具软件可视竞赛各个时间点的得分与排位，赛后工作汇报、互相交流心得，受益匪浅。特别是对作为处理对象的医学数据、影视评分数据的认识更加深刻，k-匿名、Hamming 值、差分隐私等专业知识在实践中的应用有了较深体会，同时深深地理解的数据有用性与安全生兼顾的重要性与必要性。这将为接下来的科研和职业生涯打下坚实基础，可以大幅提升研究生在信息安全领域的综合能力，推动其科研和创新能力的发展。

## 参 考 文 献

[1] Zhao F, Wu W, Feng X, et al. Physical activity levels and diabetes prevalence in US adults: findings from NHANES 2015–2016[J]. Diabetes Therapy, 2020, 11: 1303-1316.

[2] Centers for Disease Control and Prevention (CDC). National health and nutrition examination survey data[J]. Hyattsville, MD: US Department of Health and Human Services, Centers for Disease Control and Prevention, 2010, 2020.

[3] Takao Murakami, Hiromi Arai, Koki Hamada, Takuma Hatano, Makoto Iguchi, Hiroaki Kikuchi, Atsushi Kuromasa, Hiroshi Nakagawa, Yuichi Nakamura, Kenshiro Nishiyama, Ryo Nojima Hidenobu Oguri, Chiemi Watanabe, Akira Yamada, Takayasu Yamaguchi, and Yuji Yamaoka, "Designing a Location Trace Anonymization Contest ", Proceedings on Privacy Enhancing Technologies (PoPETs), vol. 2023, no. 1, pp.225-243, 2023.

[4] Murakami T, Arai H, Hamada K, et al. Designing a location trace anonymization contest[J]. arxiv preprint arxiv:2107.10407, 2021.

[5] https://www.iwsec.org/pws/2022/cup22.html

[6] Balon T, Baggili I. Cybercompetitions: A survey of competitions, tools, and systems to support cybersecurity education[J]. Education and Information Technologies, 2023, 28(9): 11759-11791.

[7] Švábenský V, Čeleda P, Vykopal J, et al. Cybersecurity knowledge and skills taught in capture the flag challenges[J]. Computers & Security, 2021, 102: 102154.

[8] Chung K, Cohen J. Learning obstacles in the capture the flag model[C]//2014 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 14). 2014.

[9] "Dataset and Lessons Learned from the 2024 SaTML LLM Capture-the-Flag Competition." arXiv Preprint, 2024.

[10] 吕倩,许昱玮,程光,等. 新工科背景下网络空间安全专业建设之路初探 [J]. 网络空间安全, 2020, 11 (08): 119-125.

[11] Okajima K, Chida K. A Study on Anonymization Through Participation in iPWS Cup 2023[C]//International Workshop on Security. Singapore: Springer Nature Singapore, 2024: 297-306.

[12] 宋晓峰,韩鹏,倪林,等. 学科竞赛和专业认证联合驱动的网络安全人才培养质量提升方法研究 [J]. 计算机教育, 2022, (04): 1-4.

DOI:10.16512/j.cnki.jsjjy.2022.04.036.

[13] 任奎,韩劲松,单珏慧. 以赛促建 以点带面 构建网络空间安全教育“专普融合”新模式 [J]. 中国信息安全, 2022, (01): 32-35.

[14] 吴淮,吉家成,詹文翰. 基于信息安全竞赛的实验课程探索与实践 [J]. 实验技术与管理, 2018, 35 (06): 174-178. DOI:10.16791/j.cnki.sjg.2018.06.043.

[15] 王亚文,喻钧,刘智平. 基于学科竞赛平台的信息对抗技术专业人才培养模式实践 [J]. 实验室研究与探索, 2018, 37 (03): 232-234.