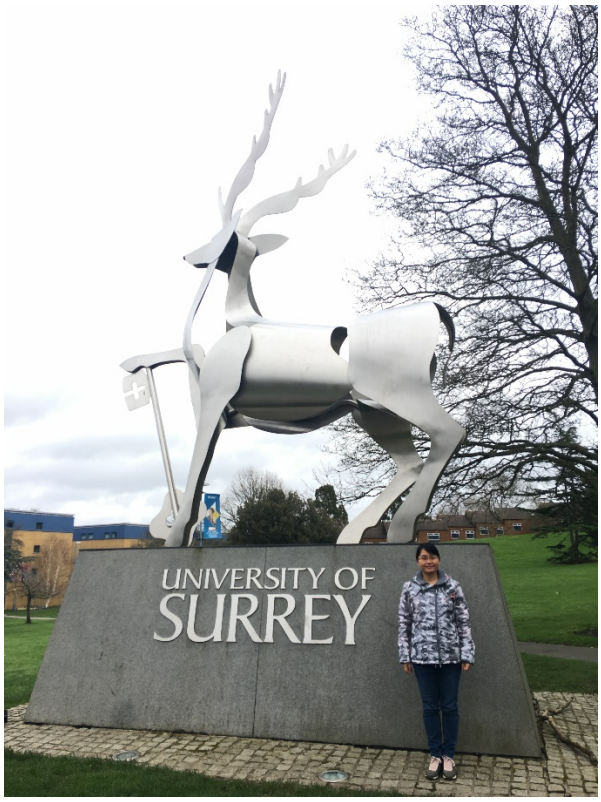
胡冬萍英国萨里大学（University of Surrey）研修总结

受学校资助，2019 年 2 月到 2020 年 2 月我在英国萨里大学(University of Surrey)计算机系进行为期一年的访学。访学期间，主要从事云存储中高效的可搜索加密方案构造的研究工作并与萨里大学计算机系的教授和学者们就所研究的课题进行了交流和探讨。同时为了获得第一手的教学信息，旁听了该系网络信息安全类的本科生课程和硕士研究生课程教授的课程。在这一年的访学生活中，感受了不同的学术研究氛围及教学方法，现对此次访学的学习经历总结如下。

一、 萨里大学总体情况

萨里大学是英国著名公立综合性研究型大学，成立于 1891 年，前身为伦敦的巴特西理工学院，1966 年 9 月 9 日被皇家许可而成为综合性大学。校区位于英格兰东南的萨里郡吉尔福德，距伦敦 30 分钟车程。萨里大学是世界著名的人工智能、移动通信和卫星空间技术研究中心，也是所有英国大学中自 1497 年以来唯一拥有英国皇室颁发的电子工程皇家教授席位（Regius Professor of Electronic Engineering）的大学。

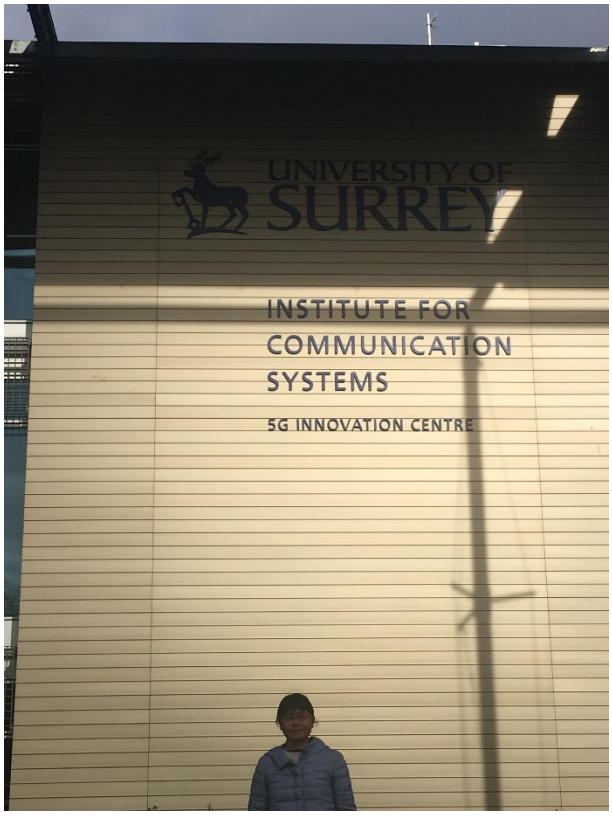
作为英国学术机构的最高荣誉，女王周年奖一共颁发过 12 次，而萨里大学就获得过其中的 4 次。该校设有七个学院，分别开设以下本科和研究生课程：文科、生物医学与生命科学、电子



学与物理学、工程学、保健与医学科学欧洲研究院、电子学、计算机与数学、表演艺术、人文科学和管理学，共有 9300 名本由大学拥有并开发的萨里研究园为超过 110 间从事各种科研，开发及设计活动的公司提供良好设施及配套。

此外，萨大在人工智能和计算机视觉领域有世界领先的研究实力。成立于 1986 年的萨里大学视觉、语音和信号处理研究中

心主要从事计算机视觉、数字信号处理、机器学习和人工智



能、计算机图形学和人机交互、医学图像处理和多媒体通信领域的研究。 科生与研究生在校学习。

萨里大学在小卫星有着广泛的研究，是全球两所拥有 5G 研发中心的大学之一。5G 创新中心（5GIC）为十多家跨国电信公司（英国电信，沃达丰，三星等）赢得了 4000 万英镑的资金，萨大受第三方资助的金额在所有英国大学中位居第三。

萨里大学图书馆藏书超过 400,000 册。图书馆内设有一百多台计算机工作站和九百多个自习座位。辅助技术中心在图书馆的一楼开放。中心内设具备特殊需要技术的工作站，例如思维图谱描绘和诵读困难学生的拼写测验。馆藏丰富、功能齐全，为师生提供全面、周到的服务。

二、访学总体情况

此次访学的合作导师是萨大计算机系的陈利群教授。陈教授在国际信息安全界具有极高的声誉，她是信息安全国际标准化组织 ISO/IEC JTC1/SC27 的资深学者，曾担任 12 个国际学术会议程序委员会主席，是四个信息安全界国际顶级学术期刊(IEEE Transactions on Information Forensics and Security, IEEE transactions on Vehicular

Technology, International Journal of Information Security and The Computer Journal）的副主编。

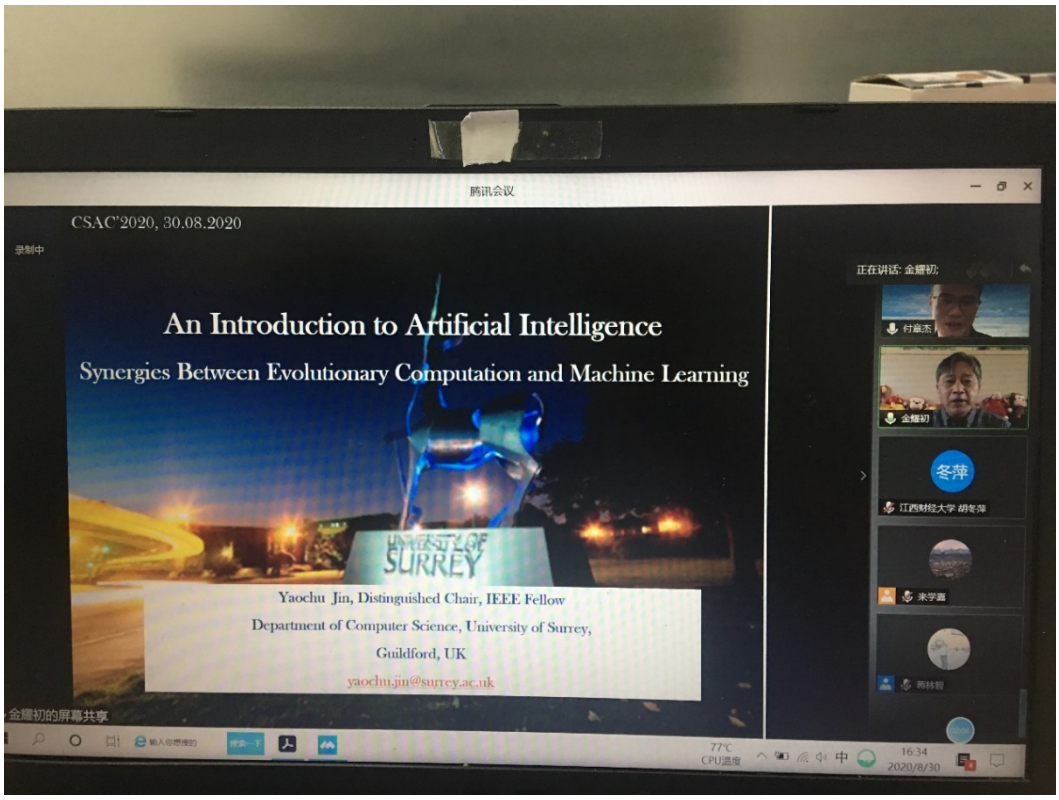
入职英国萨里大学之前，陈教授是英国惠普实验室（位于布里斯托）的信息安全首席科学家。她的突出贡献在于其主导和设计在可信计算安全界具有重要意义的直接匿名认证（Direct Anonymous Attestation, DAA）协议，这已经成为可信计算组织 TCG 和 ISO/IEC 国际标准，并已在众多的可信平台模块（TPM）上应用，该系列成果最早发表于 ACM CCS 2004，获得 2014 年 ACM CCS 测试时代大奖。此外陈教授设计的基于身份的密钥封包机制（Identity-based Key Encapsulation Mechanism，IB-KEM）成为 ISO/IEC 和 IEEE 国际标准。

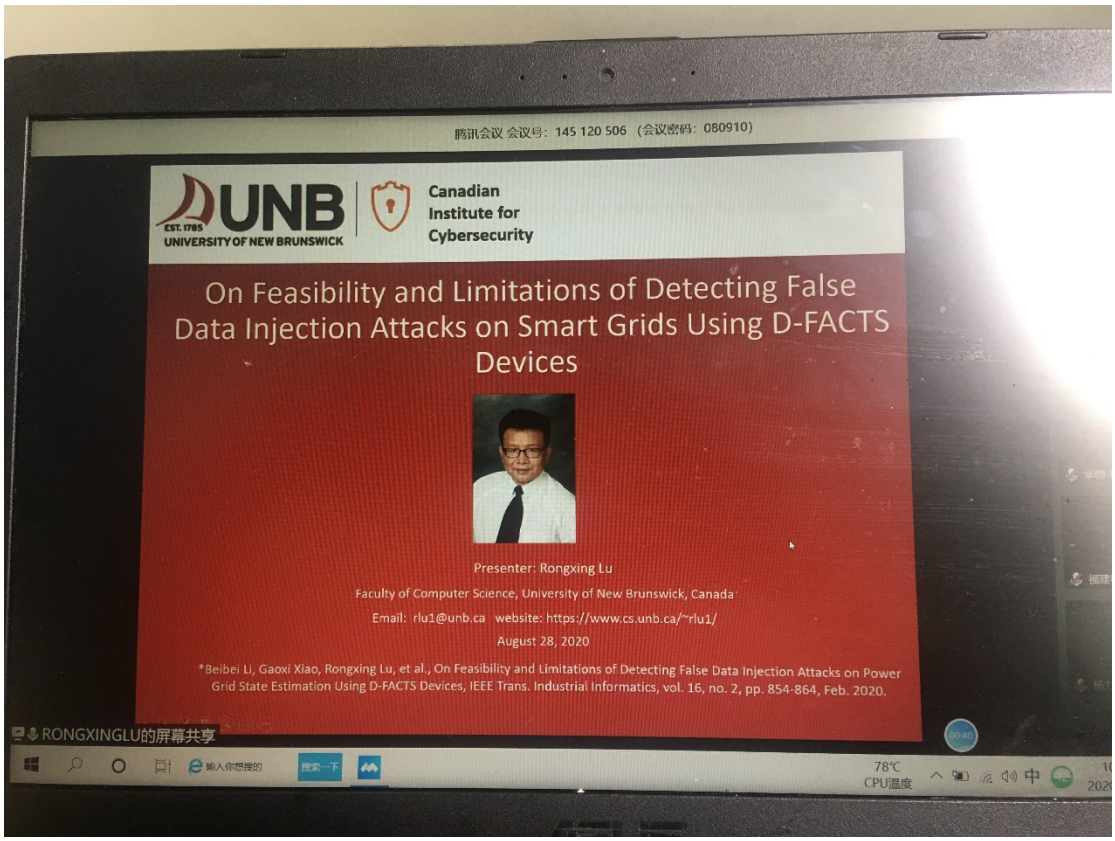
本人于当地时间 2019 年 2 月 28 日到达吉尔福德，随后到

萨大计算机系报道，与陈教授见面，详细介绍了我访学时间内的研究计划和想法，陈教授认真的与我商讨我的研究计划，随后向我介绍了信息安全团队的研究人员和系行政人员。系里在我来前就提前为我安排了工位，提供了良好的办公条件。

在访学期间，主要就我主持的国家自然科学基金课题展开研究工作。查阅国外关于云安全存储和可搜索加密等方面的研究文献，总结国内外相关理论，和萨大信息安全团队成员共同探讨网络信息安全、云加密存储与计算等研究的前沿问题。在此过程中得到陈利群教授的大力扶持与悉心指导。我们就如何构造高效的可搜索加密体制、可搜索加密方案构建中的关键问题进行了广泛探讨与深入交流，每月与陈教授开会，讨论课题进展及碰到的问题。同时积极参与计算机系信息安全课题组每周五举行的研讨会，研讨会上有一位老师或博士生分享近期研

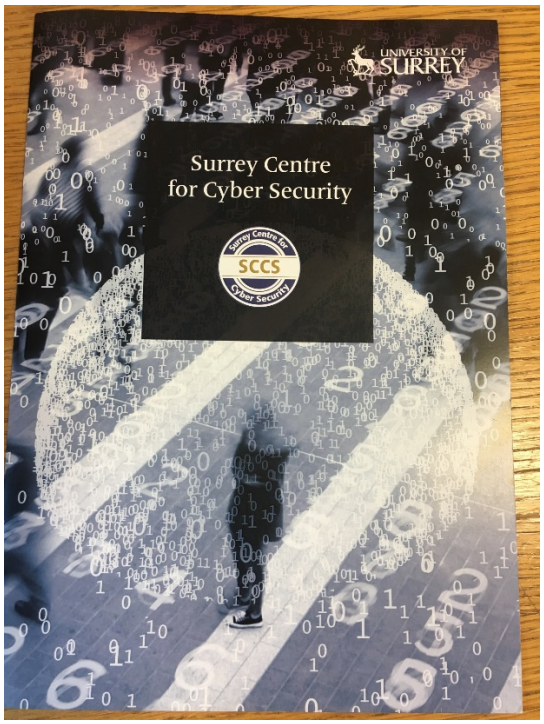
究成果或正在研读的论文。课题组还时常邀请外校教授或企业技术部门工作人员来讲学，不定期组织各种学术讲座。





访学期间深切感受到了萨里大学浓郁的学术氛围和丰富的科研活动。在与信息安全课题组师生的交流中我也有非常大的收获，能够面对面地感受到来自西方世界对网络信息安全发展认知、看法与理解，将有益于我今后的进一步学术研究工作。

科研方面的另一个收获是萨里大学信息安全团队中的团队合作非常好。团队成员里经验丰富的老师会主动帮扶年轻的老师或者博士生，每篇论文都是共同合作完成，有分工有合作，效率较高。这对研究团队建设和学科发展都会有更好的推动。博导们经常鼓励或带博士生共同参会，全心全意指导学生提升科研能力，为学生创造各种对外交流的机会，对学生的生活也关心较多，师生关系非常和谐，团队氛围很友好。



三、教学学习与交流情况

在访学期间，我旁听了网络信息安全的 2 门课程，其中一门是研究生课程《Secure Systems and Applications》、一门是本科生课程《Computer Security》。旁听后对萨里大学的教学模式有了一定了解。

Case study: Creating trust from a 'TAPESTRY' of everyday signals

"The first challenge is to understand what makes up a person's online presence, which can include interactions on social media and with many different IoT devices."
– Dr Mark Manulis

Online fraud and scams currently cost the UK economy around £670m each year, with crimes often perpetrated through false identities, so there is an urgent need for people and services to be able to provide proofs of trust in order to interact safely in the Digital Economy.

The aim of the TAPESTRY (Trust, Authentication and Privacy over a DeCentralised Social Registry) project is to investigate, develop and demonstrate new technologies that will enable people, businesses and digital services to connect safely online. A collaboration between Surrey and the Universities of Dundee and Northumbria, and a number of industry and government partners, the project explores the complex 'tapestry' of signals woven by people's everyday digital interactions: their 'digital personhood'.

"The first challenge is to understand what makes up a person's online presence, which can include interactions on social media and with many different IoT devices," explained Dr Mark Manulis of SCCS. "People and businesses need to build the trust of other users but at the same time, their privacy must also be protected."

The solution being developed in the TAPESTRY project will use cryptographic protocols to securely collect trust evidence within distributed ledgers with no central control (such as Blockchain). The idea will be that users 'opt in' to the service in order to provide evidence to verifiers for a given time period and a given granularity. One concept being explored in the project is 'zero knowledge proofs' which would, for instance, enable a verifier to prove that they are over 18 without disclosing their date of birth.

TAPESTRY is being led at Surrey by academics within SCCS, CVSSP (the Centre for Vision, Speech and Signal Processing) and the 5G Innovation Centre.

Case study: Privacy-preserving authentication in smart vehicle communications

Smart vehicles are expected to significantly improve driving experience and increase safety on public roads, as well as opening the door to new applications requiring communication between vehicles and their environment.

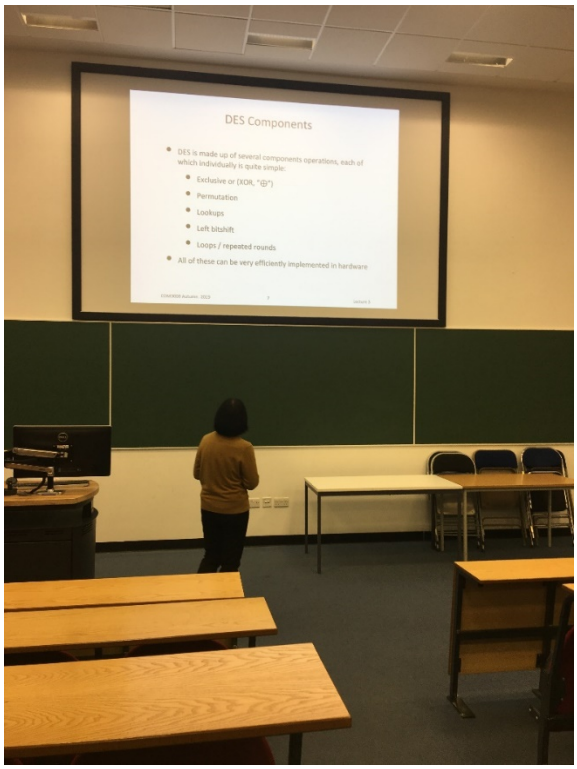
However since many of the applications envisioned for smart vehicles – such as collision avoidance and traffic management – are safety critical, it is vital that these communications are authenticated. Privacy is also a major concern because the ability to track smart vehicles could lead to profiling of drivers.

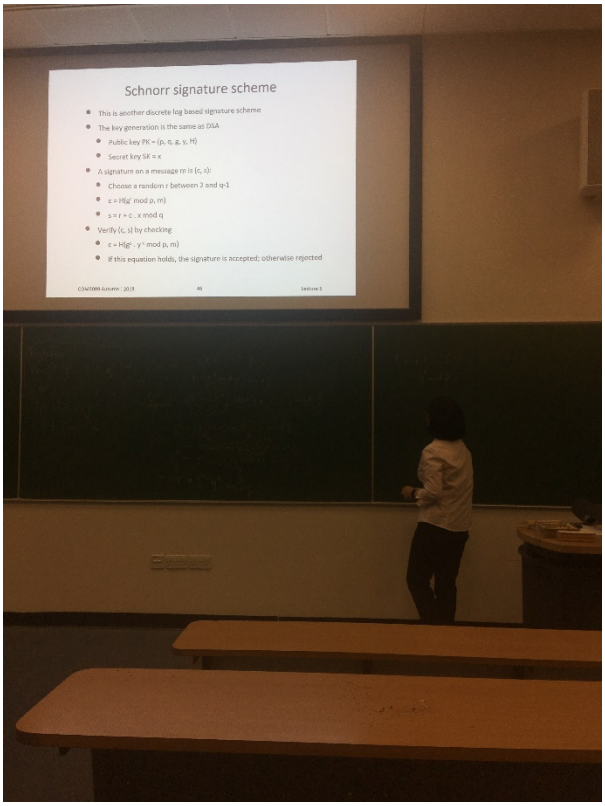
This project is developing new protocols for authentication in smart vehicle communications, based on novel attribute-based signatures. These signature schemes will potentially offer a more effective solution than existing schemes, which rely on pseudonyms, and are known to have scalability limitations as well as privacy concerns.

7

在萨里大学，无论是本科生还是硕士研究生课程，老师在开课前就会给学生提供详细的教学大纲和教学计划，包括需要学生准备汇报的问题题目和汇报的要求。同时老师还会提供阅读书目和文章的列表，提前告知要预习和课后作业。课程讨论氛围很好。硕士研究生课程时长 3 小时，2 小时老师讲授，1 小时讨论和答疑，学生发言非常积极，各种碰撞和启发，和授课老师就感兴趣的问题提问和解答，讨论，同学们非常积极和活跃。在教学过程中，授课老师会面对面和班上每一位同学进行

沟通交流，每位同学的沟通时间至少是一小时。





沟通是为了了解学生对本门课程学习过程中的建议和意见，解答学生在学习过程中的疑问。如果学生对本领域感兴

趣，愿意做更多的学习，那么老师就会尽可能提供机会，让学生进入项目中做一些力所能及的事情。本科生课程，老师讲授时间相对多一些，但每堂课都预留讨论时间，几乎本科生的每门专业课都配有实验课时，授课老师现场指导解答学生的上机问题，整个学期有 2-3 次的小组作业讨论和汇报时间。学生提交作业很守时，对老师开学初时制定的各项规则遵守度很高，对本专业的学习热情很高，而且学生很有自信。

学校校园环境很美，从教学区到学生宿舍有专门的公交车通勤，很方便。学生除了可以选修本专业的课程外，还可以选修自己感兴趣的其他专业课程，如广播、戏剧、生命科学等等。本科生的课外活动很多，很丰富，社团很活跃会定时组织各种的慈善活动，目标是塑造学生为社会服务的公益意识，这些活动里学生的参与度较高而且认真对待。


STARBUCKS COFFEE