中国科学院大学

University of Chinese Academy of Sciences

博士学位论文

基于 TPM 2.0 的协议设计与分析研究

作者姓名：王微谨

指导教师：冯登国 研究员 中国科学院软件研究所

学位类别：工学博士

学科专业：计算机应用技术

培养单位：中国科学院软件研究所

2019 年 6 月

Design and Formal Analysis of TPM 2.0 based Trusted Computing Protocols

A Dissertation submitted to the
University of Chinese Academy of Sciences
in partial fulfillment of the requirement
for the degree of
Doctor of Engineering
in Technology of Computer Application

By

Weijin Wang

Supervisor: Professor Dengguo Feng

Institute of Software, Chinese Academy of Sciences

June, 2019

中国科学院大学
学位论文原创性声明

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工作所取得的成果。尽我所知，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研究成果。对论文所涉及的研究工作做出贡献的其他个人和集体，均已在文中以明确方式标明或致谢。本人完全意识到本声明的法律结果由本人承担。

作者签名：

日　　期：

中国科学院大学
学位论文授权使用声明

本人完全了解并同意遵守中国科学院大学有关保存和使用学位论文的规定，即中国科学院大学有权保留送交学位论文的副本，允许该论文被查阅，可以按照学术研究公开原则和保护知识产权的原则公布该论文的全部或部分内容，可以采用影印、缩印或其他复制手段保存、汇编本学位论文。

涉密及延迟公开的学位论文在解密或延迟期后适用本声明。

作者签名：　　导师签名：

日　　期：　　日　　期：

摘 要

本文是中国科学院大学学位论文模板 ucasthesis 的使用说明文档。主要内容为介绍 LaTeX 文档类 ucasthesis 的用法，以及如何使用 LaTeX 快速高效地撰写学位论文。

关键词： 中国科学院大学，学位论文，LaTeX 模板

Abstract

This paper is a help documentation for the LaTeX class ucasthesis, which is a thesis template for the University of Chinese Academy of Sciences. The main content is about how to use the ucasthesis, as well as how to write thesis efficiently by using LaTeX.

Keywords: University of Chinese Academy of Sciences (UCAS), Thesis, LaTeX Template

目 录

图形列表

表格列表

符号列表

字符

Symbol	Description	Unit
R	the gas constant	$m^2 \cdot s^{-2} \cdot K^{-1}$
C_v	specific heat capacity at constant volume	$m^2 \cdot s^{-2} \cdot K^{-1}$
C_p	specific heat capacity at constant pressure	$m^2 \cdot s^{-2} \cdot K^{-1}$
E	specific total energy	$m^2 \cdot s^{-2}$
e	specific internal energy	$m^2 \cdot s^{-2}$
h_T	specific total enthalpy	$m^2 \cdot s^{-2}$
h	specific enthalpy	$m^2 \cdot s^{-2}$
k	thermal conductivity	$kg \cdot m \cdot s^{-3} \cdot K^{-1}$
S_{ij}	deviatoric stress tensor	$kg \cdot m^{-1} \cdot s^{-2}$
τ_{ij}	viscous stress tensor	$kg \cdot m^{-1} \cdot s^{-2}$
δ_{ij}	Kronecker tensor	1
I_{ij}	identity tensor	1

算子

Symbol	Description
Δ	difference
∇	gradient operator
$\delta^{\pm}$	upwind-biased interpolation scheme

缩写

CFD	Computational Fluid Dynamics
CFL	Courant-Friedrichs-Lewy
EOS	Equation of State
JWL	Jones-Wilkins-Lee
WENO	Weighted Essentially Non-oscillatory
ZND	Zel’dovich-von Neumann-Doering

第 1 章　引言

随着计算机技术和网络的迅猛发展，信息技术已经深刻改变社会的管理方式和人们的生活方式。可以说信息已经成为国家、企业和个人的重要资产，因此，保证信息的安全对于个人、企业乃至国家战略都是至关重要的。然而在利益的驱使下，针对计算机平台和网络的攻击层出不穷，使得政府、企业和个人都疲于应对。传统的信息安全保障手段主要以防火墙、入侵检测和病毒防范为主，都是以保护服务器和网络设备为主，而不重视终端的保护。而且防护的手段主要是采取封堵的办法，即捕捉滞后的特征信息，不能科学预测可能的攻击和入侵，难以抵御持续变化和迅速增长的威胁和攻击。因此，有必要从底层采取措辞来提高计算机的安全防护能力，从源头上解决人与程序、人与机器还有人与人之间的信任问题，从而有效解决信息系统的安全威胁。

可信计算的思想就是由此产生，通过在硬件层面引入安全模块，基于密码技术建立信任根、安全存储和信任链机制建立计算机系统的整体安全。经过多年的发展，可信计算技术已经不仅仅局限于传统的计算平台和环境，在移动、虚拟等平台以及与云计算、物联网等计算环境都体现出巨大的应用价值。特别是，新一代可信计算基础标准 TPM 2.0 在体系结构上与前代相比进行了革新，明确了其对移动和虚拟话平台的支持。由于新版 TPM 2.0 标准安全性并未得到充分认证，对可信计算技术的理论分析研究和推广应用也就重新燃起需求。

1.1　研究背景

信息技术的飞速发展使得各类计算平台已经深入应用到社会、经济、军事的各个领域。广大用户在享受技术进步带来便利的同时，也面临着各类安全事件所带来的危害，如恶意代码植入，计算机病毒感染，漏洞频出，隐私数据被窃取。从国家层面来说，这类问题更为严峻，涉及国家机密和国家安全。因此，如何保证终端平台的安全是信息安全领域一个重要课题。传统的安全解决方案或采用纯软件的形态，或采用专用的硬件设备。前者很容易受到计算平台内运行的其他软件或网络通信的影响，而后者又受限于高昂的造价和不同产品的异构型限制。因此有必要引入一种新型的安全硬件，以此为基础构建安全方案，即保证其经济性，又能保持其统一性和不同厂商产品间的互操作性。

可信计算思想就是由此产生，通过在应硬件层面引入安全模块，基于密码技

术建立信任根、安全存储和信任链机制。由此建立起来的可信计算组织（TCG: Trusted Computing Group, 前身为可信计算联盟 TCPA : Trusted Computing Platform Alliance）自 2001 年起发布了一系列可信计算相关规范，其中以 PC 和服务器为主要应用环境的可信平台模块规范 TPM 1.2 (TCG, 2003)，详细规定了上述硬件“安全模块”的功能、软硬件接口、安全特性和实现方式。这个规范已成为了 ISO 国际标准 (ISO/IEC 11889, 2009)。为了提高平台和设备安全性，以应对当下多变的平台环境以及安全需求，TCG 组织于 2013 年正式发布 TPM 2.0 版本草案，并于 2014 年 10 月 30 日发布 TPM 2.0 正式版 (TCG, 2014)，ISO/IEC 组织随后于 2015 年将 TPM 规范版本更新至 TPM 2.0 正式版 (ISO/IEC 11889, 2015), 标志着可信平台模块正式进入 2.0 时代。

TPM 2.0 版本规范的发布也使得产业界快速向 TPM 2.0 应用迁徙，得到了普遍应用。TPM 安全芯片已经被广泛部署到 PC 机，笔记本电脑以及服务器上，芯片厂商和操作系统提供商也都明确表示对 TPM 2.0 的支持，比如 Intel Skylake 平台已经全面支持 TPM 2.0 应用；微软 Window 10 操作系统也加强了可信计算技术的应用，充分利用 TPM 进行访问控制和身份认证；Linux Kernel 4.0 起也开始支持 TPM 2.0 驱动；IBM 也已经发布了 TSS 2.0 中间件。国内各大硬件厂商（比如联想和国民技术等）也对 TPM 2.0 的发展与推广贡献了重要核心作用，比如 TPM 2.0 新增了对国产密码学算法的支持；同时吸收和学习了中国 TCM（Trusted Cryptographic Module）技术中广泛使用对称密码的方式以提高应用性能。

TPM 2.0 与 TPM 1.2 相比，从算法灵活性、功能多样性、平台安全性和效率等方面，有了显著的提升。比如增加了对国产算法的支持，新增了策略授权功能，加强了算法的强度以及改进了授权会话的安全性，采用更加高效的基于椭圆曲线的直接匿名证明方案。这些新增和加强的功能说明 TPM 2.0 不仅仅是从 TPM 1.2 单纯的继承过来。因此，之前针对 TPM 1.2 平台功能的安全性分析于研究并不能直接说明 TPM 2.0 的平台安全性，需要重新针对 TPM 2.0 协议和接口的安全性进行评估，以此反应新增和增强的功能是否还符合所期望定义的安全。幸运的是，虽然可信计算基础理论研究相对滞后，但是经过 TPM 1.2 的研究与发展，已经具有了一些经典的分析方式，其中形式化分析便是常用手段之一。其威力已经在 TPM 1.2 的研究与发展中得到充分体现，发现了许多漏洞与威胁，对 TPM 的发展立下了汗马功劳。因此，本文也是充分利用形式化分析方法对 TPM 2.0 的协议与协议进行研究，以期得到平台安全性的理论保障。

除了保证平台安全外，TPM 2.0 对隐私的保护的要求也在提高。TPM 在进

行远程证明的时候，需要想远程验证方证明自己是一个值得信赖的通信实体，即进行平台身份证明。最初 TCG 采用可信第三方 PrivacyCA 协助 TPM 完成身份证明，从而避免平台身份信息的直接泄漏，但是 PrivacyCA 是完全知道 TPM 的真是身份，这也在一定程度上存在隐患。基于此种缺陷，TCG 提出了直接匿名证明（DAA：Direct Anonymity Attestation）的 TPM 身份认证方法，使得平台拥有者能够直接向远程验证方证明自己的真实身份，同时又不暴露自己真实身份信息。TPM 1.2 采用了基于 RSA 算法的 DAA 协议（以下简称 RSA-DAA），TPM 2.0 采用了基于椭圆曲线双线性对的 DAA 协议（以下简称 ECC-DAA）。ECDAA 方案有着比 RSADAA 方案更加高效的运行效率，同时由于 TPM 1.2 中对 DAA 协议接口定义的高度封装性，使得其使用灵活度不高。而 TPM 2.0 中对实现 DAA 协议的接口定义灵活，不仅能够实现不同双线性对方案的 ECC-DAA 协议，甚至可以实现与 DAA 相同思想的匿名凭证类协议，使得 TPM 2.0 的应用更加广泛。本文的研究也在 DAA 协议的基础上，研究了其他类型的匿名凭证类协议。

综上所述，本课题将针对新一代可信计算技术的安全性和隐私性进行深入研究。在安全性研究方面，利用形式化分析方法对装载 TPM 2.0 技术的可信计算安全芯片提供的授权会话、密码功能支撑命令等接口的安全性进行形式化分析；在隐私性方面的研究，在深入了解 DAA 协议的基础上，研究无可信第三方的匿名凭证类协议和系统。特别是这类协议所具有的匿名黑名单功能，可以促进 DAA 协议的应用延伸。反之，针对 DAA 协议的形式化分析方法，亦可以进行改进与发展，使之适应于含有匿名黑名单机制的匿名凭证协议，发现其漏洞并加以改进。最后，基于 TPM 2.0 的接口，我们还能实现这类匿名凭证协议。本课题的研究意义在于：

（1）无论是国外还是国内，在可信计算领域都处于技术超前于理论，理论滞后于技术的状况。可信计算的理论研究落后于技术的开发。进行可信计算安全性分析理论和方法的研究，可以推进可信计算理论研究的发展。

（2）对可信计算协议与接口进行安全性分析，结合其应用场景，给出安全评估，改进在应用场景的安全性，有利于可信计算技术的推广与应用。

（3）对匿名凭证类系统的研究，有利用 DAA 协议的发展与应用。

（4）结合我国信息安全管理的国情，推进可信计算芯片的本土化进程，为我国新一代可信计算的设计与分析提供借鉴。

1.2 研究现状

本文研究基于 TPM 2.0 的协议，可以粗略的分为两个层面的协议：一是基于芯片的基础接口组合协议，定义了可信计算安全芯片的安全机制，例如密钥管理、授权认证、密码学支撑服务（加密、签名等）等接口组合协议。二是基于调用这些基础接口实现的更为复杂的协议，例如直接匿名证明协议和匿名凭证方案等。本节分三个维度介绍课题相关的研究现状，分别是安全协议形式化分析方法、可信计算基础协议和接口的安全性分析以及可信计算延伸协议的设计与分析。

1.2.1 安全协议形式化分析方法研究现状

形式化分析方法在开发一些注重安全和保障的关键系统上，逐渐地引起广泛的关注。在安全协议这个领域尤其得到了体现。一些重要的安全协议，比如安全传输层协议 TLS 以及它的前任安全套接层协议 SSL，出现细微的缺陷都会导致巨大的经济损失。因此在设计协议的时候保证其安全性显得尤为重要。而形式化方法就是对安全协议的安全性进行分析验证，从而克服人为证明的易错性。

一般公认，Needham et al. (1978) 最早提出了安全协议形式化分析的思想，但其主要工作仅仅是建立了 Needham-Schroeder 协议。而第一个用形式化方法对协议进行分析的文章，当属Dolev et al. (1981) 在 1981 年的结果，建立了验证协议安全性的 Dolev-Yao 模型。他们用算法的手段分析了两类特殊的协议的安全性。随后的Dolev et al. (1983) 的分析方法与之一脉相承，都是用多项式时间的算法对于某些特定类型协议的安全性进行判定。此外，基于 Dolev-Yao 模型的模型检测工具也相继开发出来，例如 Interrogator(Millen et al., 1987) 和 NRL 协议分析器 (Meadows, 1994) 等。

Dolev-Yao 模型提出之后，形式化方法又一里程碑的工作是由Burrows et al. (1989) 提出的 BAN 逻辑，他们利用知识和信念逻辑，描述和推理认证协议。沿着这个方法，许多逻辑被构造了出来，其中大部分是 BAN 逻辑的变种。BAN 逻辑之后出现的较为新颖的定理证明技术，包括了 Paulson 归纳法 (Paulson, 1998)、串空间 (Fábrega et al., 1998)、类型检测 (Abadi, 1999; Gordon et al., 2003) 和其他方法 (Kemmerer et al., 1994; Dutertre et al., 1997) 等。根据这类定理证明技术开发的定理证明器如 PVS(Owre et al., 1992) 和 Athena(Song et al., 2001) 等。

在上述这些基于 Dolev-Yao 模型（以下简称符号模型）的形式化分析方法和工具蓬勃发展时机，另外一种基于计算复杂性模型（以下简称计算模型）的形式

化方法也悄然形成。一种为间接方式，即通过证明基于 Delve-Yao 模型的形式化方法的计算可靠性，从而得到形式化分析的可证明安全结论。另一种为直接方式，即基于游戏序列的证明技术，通过进程演算语言描述协议，从而直接得到协议的可证明安全结论。

因此，从敌手模型类型进行分类，可以将形式化分析分为符号模型下的形式化方法和计算模型下的形式化方法。由于形式化分析方法呈现“百家争鸣”的景象，本课题着重研究了两种敌手模型下部分的形式化分析方法。下面介绍的形式化分析方法的发展现状是与本课题研究内容相关的：基于符号模型的形式化方法和基于计算模型的形式化方法。

1.2.1.1 基于符号模型的形式化分析方法现状

基于标准 Pi 演算语言 (Milner, 1999)，Abadi et al. (2001, 2017) 于 2001 年提出了应用 Pi 演算的概念，与Abadi et al. (1997) 提出的 spi 演算的主要不同之处体现在对密码原语的操作上，spi 演算内建固定原语，而应用 Pi 演算利用等价理论，可以支持自定义的更多复杂的原语。此外，应用 Pi 演算的出现也促进了自动化分析工具的发展。

2001 年，Blanchet (2001) 提出了一个基于 Prolog 规则的协议分析器，用于分析协议的机密属性。协议由 Prolog 规则表示，并且用一个高效的算法确定某一事实是否能从这些规则（知识）中推导出来。2002 年，Abadi et al. (2002, 2005) 开发了两个协议分析技术，一个基于应用 Pi 演算的类型检测进程语言，一个基于无类型的逻辑程序（Prolog）。并且证明了两种技术的等价性。从而给出了从应用 Pi 演算建模的进程语言到逻辑语言的转化，提出了协议自动验证工具 Proverif。Proverif 工具将协议用基于应用 Pi 演算的进程语言表述，然后转化为 Horn 字句的表示，最后利用这些 Horn 语句（包括协议和敌手能力等），用可达性理论来求解某一个事实是否可达（证明机密属性）。与模型检测方法相比，Proverif 没有了状态空间爆炸的问题。然而，Proverif 不是完备的，它会产生错误攻击。但是实验表明错误攻击极少出现，分析成功率高，因此该工具得到了广泛应用，例如 (Blanchet et al., 2008a; Bhargavan et al., 2017)。

随后，基于应用 Pi 演算和 Proverif 的研究工作越来越多。其中，Blanchet 等人继续扩展 ProVerif 支持的安全属性，包括对应性（可证明协议的人这个属性）(Blanchet, 2002, 2009)、强机密性 (Blanchet, 2004)、选择项等价 (Blanchet et al., 2005)。然而选择项等价的假设是强于观察等价的，因此只适用于证明一类等价

关系，即两个进程为同一进程的不同版本，仅选择的项不同。为了使 ProVerif 支持更多的等价关系，Cheval et al. (2013) 通过定义项的重写规则，使之可以支持含有条件分支的等价关系。Blanchet et al. (2016) 也拓展了选择项等价，使之可以证明需同步的两个进程间的等价关系。

还有一部分的工作集中在对应用 Pi 演算和 ProVerif 的扩展上，Arapinis et al. (2011) 在 ProVerif 的基础上，加入全局状态补丁，使之可以分析代全局状态的协议，并且命名为 Statverif；之后他们同步跟进了对应用 Pi 演算理论的全局状态扩展 (Arapinis et al., 2014)。另外一个基于应用 Pi 演算进行全局状态扩展是Kremer et al. (2016) 开发的分析有限状态协议的 SAPIC 工具，该工具的协议表达为基于应用 Pi 演算的进程语言，然后转化为多重集重写规则，再借助 Tamarin 工具 (Schmidt et al., 2014) 进行分析。同时，作者证明了工具的完备性。

Paiola et al. (2012) 提出了一种使用有限长度列表建模和分析无限长度列表的协议的方法，然而他们协议建模语言是广义上的 Horn 子句，还不能用 ProVeif 语言建模，因还不支持 ProVerif 进行自动分析。Chothia et al. (2015) 提出在进程中插入“阶段”，避免一类由 ProVerif 分析私密性而产生的错误攻击，比如分析承诺协议中的私密性。目前 ProVerif 仅实现了在非复制进程中插入“阶段”进行分析。

1.2.1.2 基于计算模型的形式化分析方法现状

自从Abadi et al. (2000) 提出在某种情况下，Dolev-Yao 模型下的安全性定义蕴含计算模型下的安全性定义，许多工作开始热衷于关联两种模型的研究。这些工作的结果给出了在 Dolev-Yao 模型下的计算可靠性，例如 (Backes et al., 2003; Cortier et al., 2005; Janvier et al., 2005)。这些工作大都没有实现自动化证明。之后出现利用 Dolev-Yao 模型的自动化工具证明协议的安全性，再利用定理证明其计算可靠性，例如 (Canetti et al., 2006)。一个比较系统的工作是由Backes et al. (2009) 提出的通用证明框架 CoSP（Computatioanl Soundness Proofs），该框架能够在符号模型下进行计算可靠性证明，将密码学原语证明和形式化演算分离开进行模块化证明。因此 CoSP 框架特别适合证明形式化演算类工具的计算可靠性证明。基于 CoSP 框架，其作者进行了一系列的后续研究工作，例如利用该通用框架证明了形式化分析工具 F7(Backes et al., 2010) 和 ProVerif(Backes et al., 2014) 的计算可靠性结果。Shao et al. (2016) 也利用此框架证明了带状态的应用 Pi 演算的计算可靠性。

上述这些研究都是属于采用间接方式的到计算可靠性结果。由于符号模型

和计算模型不可能精确对应，有的为了其证明方法的可靠性需要额外的假设，其因此这类的结果总有其限制性。基于此，学者开始考虑直接利用形式化方法来证明协议的计算可靠性，从而绕过符号模型。2005 年，Halevi (2005) 讨论了利用游戏序列证明技术实现自动化证明工具的可行性。2006 年，Bellare et al. (2006) 实现基于代码的游戏序列证明框架，并且利用该框架证明了 3-DES 对称加密算法。

一个比较系统的工作是由Blanchet (2006, 2008) 设计和实现的在计算模型下的全自动证明工具 Cryptoverif，该工具利用概率多项式的进程演算语言来表示协议，利用游戏序列组织证明协议的机密属性。翌年，Blanchet 扩展 Cryptoverif(Blanchet, 2007)，使其支持证明认证属性。该工具已经成功证明许多协议，比如 Yahalom 协议、Needham-Schroeder 协议、Kerberos 协议 (Blanchet et al., 2008b)、SSH 协议 (Cadé et al., 2013) 和 TLS 1.3 协议 (Blanchet, 2018)。

另外一个系统的工作是由Barthe et al. (2011) 设计的在计算模型下自动化验证工具 EasyCryp（其前身 CertiCrypt(Barthe et al., 2009)），该工具也是基于游戏序列证明协议，其提供的自动化证明方式为从一个协议的证明骨架去自动化补全或者说详细阐述为一个完整的 Game 序列证明过程。因此，其与 Cryptoverif 相比更注重验证性，即 EasyCrypt 需要使用者先提供证明的框架，然后它进行完善及验证该框架的正确性。

Blanchet 团队还有一个工作计划是将 ProVerif 和 CryptoVerif 的输入脚本语言统一，这样一份协议的输入脚本可以同时验证其在符号模型下的安全性，也可以得到在模型下的可安全性证明，达到优势互补的目的。该项工作目前取得了突破进展，在最新发布的 ProVerif 2.0 和 CryptoVerif 2.0 已经实现大部分输入语言的兼容。这方面典型的分析工作是 ARINC823 公钥和分享密钥协议 (Blanchet, 2017)。这两个协议是航空协议，用于空对地交流。

1.2.2 可信计算基础协议和接口的安全性分析现状

在过去的几年中，许多可信计算基础协议和接口（全称为应用程序接口，Application Programming Interface，以下描述有时也称做 API 接口）的缺陷被发现，这些问题大都与机密性和认证性相关。在发现攻击和漏洞的过程中，形式化分析方法扮演了重要的角色。而且随着形式化方法的发展，匿名性和其他各类高级安全属性也逐渐被描述出来。因此形式化分析方法的应用范围也更加广阔，包括应用于新一代可信计算平台 TPM 2.0 协议和接口的分析中。下面就近年来可信计算平台（包括 TPM 1.2 等早期版本）基础协议和接口分析现状做一个简要

的概述。

Lin (2005) 利用定理证明器 Otter 和 Alloy 分析了 TPM 1.2 的大量接口组合，他的分析结果包括发现授权协议中的密钥句柄转换攻击等。Bruschi et al. (2005) 证明了 OIAP 协议易受重放攻击，攻击者可以重发已执行的命令。Gürgens et al. (2007) 利用有限状态自动机分析了 TPM 1.2 的 API 接口组合，发现在远程证明的证书申请过程中，攻击者可以非法获得其选择密钥的证书。Datta et al. (2009) 设计了一种安全系统逻辑，并分析了 TPM 完整性收集和报告功能，发现攻击者可以任意修改 PCR 值，破坏信任链传递机制。Chen et al. (2009b) 发现了一个对授权数据的离线字典攻击，而后又给出了共享授权数据的应用场景下中间人攻击的问题 (Chen et al., 2009a)。Delaune et al. (2010) 利用 Proverif 工具分析了 TPM 1.2 部分 API 接口，但是忽略了 PCR 状态。随后他们又分析了基于 PCR 状态的认证协议建模方法 (Delaune et al., 2011)，扩展了 Proverif 分析范围。

随着 TCG 组织发布 TPM 2.0 标准，一些基于 TPM 2.0 协议和 API 的分析也随后出现。Shao et al. (2013) 利用类型检测系统分析了 TPM 2.0 的存储保护部分。Zhang et al. (2014) 利用 Tamarin 工具分析了 TPM 2.0 密钥管理部分接口，发现并修正了在 TPM 2.0 中密钥迁徙过程中存在的攻击。Zhao et al. (2015) 分析 TPM 2.0 中 SM2 密钥交换协议，发现由于 TPM 2.0 的接口设计，其还是存在未知密钥攻击和密钥泄漏伪装攻击，并提出修补方案。Shao et al. (2018) 利用有状态的应用 Pi 演算对基于 HMAC 的授权协议进行建模，并利用 Tamarin 工具分析发现在 TPM 初始化后缺少安全会话的攻击场景存在中间人攻击，导致 TPM 的调用者不能建立安全会话，并提出了修补方案。

可以看出，对应用程序接口组合的分析都是利用形式化模型下的分析工具或者分析方法，致力于寻找其可能存在的缺点和攻击。还有一个研究路线是致力于应用程序接口框架的可证明安全。Cortier et al. (2009, 2014) 提出一个对称密钥管理 API 接口框架，并且定义了一个形式化安全策略，手动证明其安全性。Daubignard et al. (2014) 应用其可证明方法扩展了该 API 接口使得支持非对称密钥管理。Cachin et al. (2009) 提出一个可证明安全的密码学 API 接口，他们利用现代密码学定义了接口的安全策略并手动证明了接口的安全性。Chu et al. (2015) 利用他们的方法，用现代密码学定义了 TPM 2.0 中密码学接口的安全策略并证明了安全性。

1.2.3 可信计算延伸协议的设计与分析现状

匿名凭证系统（anonymous credentials, 也称为 PABC，即 Privacy-enhancing attribute-based credentials）是一些注重隐私的认证系统的核心组成部分，允许用户盲申请证书（即不暴露或暴露部分属性），同时能够以不可链接的方式证明自己拥有该证书且不暴露隐藏的属性。一般认为第一个提出匿名凭证思想的是Chaum (1985)，随后一大批方案相继提出。比较流行的两个方案是 IBM 的 Identity Mixer(Camenisch et al., 2010) 和微软的 U-Prove 方案 (Paquin et al., 2011)。前者基于 CL 签名方案 (Camenisch et al., 2001, 2002, 2004)，而后者基于 Brands 盲签名 (Brands, 2000)。由于 CL 签名方案建立在 RSA 群上，Brands 盲签名建立在素数阶群上，因此 U-Prove 方案效率远高于 Mixer 方案。但是，基于 CL 签名的是一个可证明安全的方案，而 U-Prove 方法目前并没有被证明安全。而且，2013 年 Baldimtsi 和 Lysyanskaya(Baldimtsi et al., 2013b) 证明了所有已知的随机模型下可证明方法都不能证明 Brands 盲签名的安全性。同年，他们提出一种可证明安全，且效率值接近 U-Prove 的方案 ACL(Baldimtsi et al., 2013a)。2014 年，Chase 等人提出一个基于对称基础设施 MAC 方案的匿名凭证系统 (Chase et al., 2014)，与 U-Prove 和 ACL 相比，除了得到相近的效率外，还能够支持凭证的多次使用而不被链接行为。

直接匿名证明（DAA, Directed Anonymous Attestation）方案是匿名凭证方案的一种应用。第一个 DAA 协议由Brickell et al. (2004) 提出，基于 RSA 群上的 CL 方案实现，随后被 TCG 采用为 TPM 1.2 标准中，作为平台身份证明的方案，使得通讯方能够向远程验证方证明自己拥有合法 TPM，同时又避免暴露自己的真实身份信息。

随后，DAA 方案得到了快速发展，提出了一系列基于 ECC 的 DAA 方案 (Brickell et al., 2008; Xiaofeng et al., 2008; Brickell et al., 2009; Chen et al., 2009c; Brickell et al., 2010; Chen et al., 2010)。ECC-DAA 协议的效率比 RSA-DAA 更高，因此成为了 TPM 2.0 标准首选的方案。然而由于 TPM 1.2 种对 RSA-DAA 协议进行了高度封装实现，即只实现 TPM_Join() 和 TPM_Sign() 接口，不能灵活实现各类的直接匿名证明协议。因此在 TPM 2.0 标准中，并没有封装 DAA 协议接口，而是实现了基础接口，即利用密钥建立接口、承诺接口和签名接口等联合起来实现 DAA 协议。其中，Chen et al. (2010) 和Brickell et al. (2010) 提出的 ECC-DAA 方案是目前实现效率较优的方案，被 TCG 发布的 TPM 2.0 标准支持。灵活接口的实现使得 TPM 平台能够支持更多类型的匿名认证协议，比如Chen et al. (2013)

利用 TPM 2.0 提供的接口实现了 ECC-DAA 方案，也给出了对 U-Prove 方案的支持。

而在 DAA 协议分析方面，Backes et al. (2008) 首次利用应用 Pi 演算建模和分析 API 协议，发现了 DAA 协议的一个安全缺陷：攻击者可以使得匿名凭证颁发者无法精确统计已持有证书的平台。Smyth et al. (2011, 2015) 首次利用应用 Pi 演算对 RSA-DAA 和 ECC-DAA 的匿名属性进行定义，并且应用 Proverif 工具进行安全性分析。Brickell et al. (2012) 声称大部分 DAA 方案可以被恶意用户作为静态 DH 问题预言机，使得安全等级降低为原有的 2/3。Xi et al. (2014b) 利用应用 Pi 演算建立了 TPM 2.0 中用于实现 DAA 协议的应用接口模型，定义了匿名性、用户控制的可追踪性和不可陷害性等安全属性，并利用 ProVerif 获得安全性分析结果。Camenisch et al. (2016) 声称所有已知的 DAA 安全模型都是不完备或不安全的，并且给出一个在 UC 框架（Universally Composable Framework）下的安全证明模型。

DAA 协议中并没有具体指出如何撤销恶意 TPM 平台或已被攻克 TPM 平台的身份证书。一般来说，平台证书的撤销功能通过黑名单实现，当用户身份证书进入黑名单，其便不能认证通过。然而如果直接应用上述匿名凭证系统的机制，会导致匿名性遭到挑战，因为为了实现证书撤销，可信第三方势必要掌握用户的关键身份信息，因此，如果可信第三方与验证者合谋，用户的真实信息就会泄漏。基于此种考虑催生出无可信第三方的匿名凭证系统。

2007 年，Brickell et al. (2007) 率先扩展了 DAA 协议，提出了 EPID 方案，在 DAA 的基础上增加了证书撤销功能。同年，出现了类似于 EPID 思想的另一个可撤销的匿名认证系统 BLAC(Tsang et al., 2007)，这类型的匿名认证系统允许验证者直接撤销恶意用户，而不需要通过可信第三方 TTP。以及随后出现效率更高，基于累加器的匿名认证方案 PEREA(Tsang et al., 2008)。同时，基于 BLAC 和 PEREA 的匿名信誉系统 BLACR(Au et al., 2012b) 和 PERM(Au et al., 2012a) 也相继被提出。匿名信誉系统的证书撤销功能通过信誉积分来实现，信誉积分有一个阈值，当用户累计的积分超过这个阈值后，用户的证书就会被禁用。与 PERM 同年提出的基于 PEREA 的匿名信誉系统 PE(AR)^2(Yu et al., 2012)，取消了 PEREA 中时间窗口的限制，但赎回分数的方案存在着漏洞。Xi et al. (2014c) 改进了 PE(AR)2 的漏洞，提出 ARBRA 方案，但这种设计方案过于复杂。之后，Xi et al. (2014a) 设计了新的匿名信誉系统 FARB(Xi et al., 2014a)，兼顾了效率和应用规模，并声称可以运行在资源受限的移动环境中。Henry et al. (2013) 在 2013 年

通过零知识的批处理技术改进 BLACR 的效率，提出 BLACRONYM 方案。2018 年由Yang et al. (2018) 提出 DBLACR 方案继承 BLACR 的功能，利用去中心化的思想使得用户的注册过程无需第三方。

TPM 2.0 中对 DAA 协议接口的灵活性也使得 TPM 2.0 的应用更加广泛，除了在之前提到的由Chen et al. (2013) 利用 TPM 2.0 中基础 DAA 接口实现 U-Prove 方案。邵健雄 (2016) 提出的 DAA-$(AR)^2$ 方案利用 TPM 2.0 中 DAA 基础接口实现，改进 PE$(AR)^2$ 中的安全问题。这些都说明了 TPM 2.0 更加广泛的应用前景。

1.3 论文工作

1.4 论文组织

本文的后续内容安排如下：

第**??**章介绍了双系分析的攻击框架，评估了分组密码 Piccolo 以及 LBlock 算法抗双系分析的安全性。除此之外，研制了一套双系攻击的自动分析软件，用于评估给定分组密码的密钥编排的扩散特性。

第**??**章改进了已有零相关线性分析的攻击模型，更新了分组密码 LBlock 以及 TWINE 算法的安全性评估结果，以此说明密钥编排中等价密钥对分组密码安全性的影响。

第**??**章以 Zorro 算法的差分分析为例，探究了简单密钥编排下分组密码差分分析的适用性。

第**??**章主要研究了分组密码在杂凑模式下的安全性，主要包括分组密码在选择密钥假设下的互补性研究以及分组密码在已知密钥下的扩散性研究。

第**??**章深入分析了 Piccolo 算法的线性密钥编排，发现其轮常数选取方面存在的安全性隐患；以此指导简单密钥编排的设计，尤其是轮常数的选取。

第**??**章系统总结了上述几章中提炼出的分组密码密钥编排的设计准则。并针对一类特殊的密钥编排，给出了较高效的设计流程；并将此设计流程应用于 LBlock 算法。

第**??**章对全文进行总结，并对后续研究工作进行了简单介绍。

第 2 章　LaTeX 使用说明

为方便使用及更好地展示 LaTeX 排版的优秀特性，ucasthesis 的框架和文件体系进行了细致地处理，尽可能地对各个功能和板块进行了模块化和封装，对于初学者来说，众多的文件目录也许一开始让人觉得有些无所适从，但阅读完下面的使用说明后，会发现原来使用思路是简单而清晰的，而且，当对 LaTeX 有一定的认识和了解后，会发现其相对 Word 类排版系统极具吸引力的优秀特性。所以，如果是初学者，请不要退缩，请稍加尝试和坚持，以领略到 LaTeX 的非凡魅力，并可以通过阅读相关资料如 LaTeX Wikibook(Wikibook, 2014) 来完善自己的使用知识。

2.1　先试试效果

1. 安装软件：根据所用操作系统和章节 **??**中的信息安装 LaTeX 编译环境。

2. 获取模板：下载 ucasthesis 模板并解压。ucasthesis 模板不仅提供了相应的类文件，同时也提供了包括参考文献等在内的完成学位论文的一切要素，所以，下载时，推荐下载整个 ucasthesis 文件夹，而不是单独的文档类。

3. 编译模板：

(a) Windows：双击运行 artratex.bat 脚本。

(b) Linux 或 MacOS: `terminal -> chmod +x ./artratex.sh -> ./artratex.sh xa`

(c) 任意系统：都可使用 LaTeX 编辑器打开 Thesis.tex 文件并选择 xelatex 编译引擎进行编译。

4. 错误处理：若编译中遇到了问题，请先查看“常见问题”（章节 2.4）。

编译完成即可获得本 PDF 说明文档。而这也完成了学习使用 ucasthesis 撰写论文的一半进程。什么？这就学成一半了，这么简单???，是的，就这么简单！

2.2　文档目录简介

2.2.1　Thesis.tex

Thesis.tex 为主文档，其设计和规划了论文的整体框架，通过对其的阅读可以了解整个论文框架的搭建。

2.2.2 编译脚本

• Windows：双击 Dos 脚本 artratex.bat 可得全编译后的 PDF 文档，其存在是为了帮助不了解 LaTeX 编译过程的初学者跨过编译这第一道坎，请勿通过邮件传播和接收此脚本，以防范 Dos 脚本的潜在风险。

• Linux 或 MacOS：在 terminal 中运行

– `./artratex.sh xa`：获得全编译后的 PDF 文档

– `./artratex.sh x`：快速编译模式

• 全编译指运行 `xelatex+bibtex+xelatex+xelatex` 以正确生成所有的引用链接，如目录，参考文献及引用等。在写作过程中若无添加新的引用，则可用快速编译，即只运行一遍 LaTeX 编译引擎以减少编译时间。

2.2.3 Tmp 文件夹

运行编译脚本后，编译所生成的文档皆存于 Tmp 文件夹内，包括编译得到的 PDF 文档，其存在是为了保持工作空间的整洁，因为好的心情是很重要的。

2.2.4 Style 文件夹

包含 ucasthesis 文档类的定义文件和配置文件，通过对它们的修改可以实现特定的模版设定。若需更新模板，一般只需用新的样式文件替换旧的即可。

1. ucasthesis.cls：文档类定义文件，论文的最核心的格式即通过它来定义的。

2. ucasthesis.cfg：文档类配置文件，设定如目录显示为“目 录”而非“目录”。

3. artratex.sty: 常用宏包及文档设定，如参考文献样式、文献引用样式、页眉页脚设定等。这些功能具有开关选项，常只需在 Thesis.tex 中的如下命令中进行启用即可，一般无需修改 artratex.sty 本身。

```
\usepackage[options]{artratex}
```

4. artracom.sty：自定义命令以及添加宏包的推荐放置位置。

2.2.5 Tex 文件夹

文件夹内为论文的所有实体内容，正常情况下，这也是**使用 ucasthesis 撰写学文论文时，主要关注和修改的一个位置，注：所有文件都必须采用 UTF-8 编码，否则编译后将出现乱码文本**，详细分类介绍如下：

• Frontpage.tex：为论文中英文封面及中英文摘要。**论文封面会根据英文学位名称如 Bachelor，Master，或是 Doctor 自动切换为相应的格式**。

• Mainmatter.tex：索引需要出现的 Chapter。开始写论文时，可以只索引当

前章节，以快速编译查看，当论文完成后，再对所有章节进行索引即可。

- Chap_xxx.tex：为论文主体的各个章节，可根据需要添加和撰写。
- Appendix.tex：为附录内容
- Backmatter.tex：为发表文章信息和致谢部分等。

2.2.6 Img 文件夹

用于放置论文中所需要的图类文件，支持格式有：.jpg, .png, .pdf。其中，`ucas_logo.pdf` 为国科大校徽。不建议为各章节图片建子目录，即使图片众多，若命名规则合理，图片查询亦是十分方便。

2.2.7 Biblio 文件夹

1. ref.bib：参考文献信息库。
2. gbt7714-xxx.bst：符合国标的文献样式定义文件。由 zepinglee 开发，并满足最新国标要求。与文献样式有关的问题，请查阅开发者所提供的文档，并建议适当追踪其更新。

2.3 数学公式、图表、参考文献等功能

2.3.1 数学公式

比如 Navier-Stokes 方程:

$$\begin{cases} \frac{\partial \rho}{\partial t} + \nabla \cdot (\rho \boldsymbol{V}) = 0 \text{ times font test} \\ \frac{\partial (\rho \boldsymbol{V})}{\partial t} + \nabla \cdot (\rho \boldsymbol{V} \boldsymbol{V}) = \nabla \cdot \boldsymbol{\sigma} \text{ times font test} \\ \frac{\partial (\rho E)}{\partial t} + \nabla \cdot (\rho E \boldsymbol{V}) = \nabla \cdot (k \nabla T) + \nabla \cdot (\boldsymbol{\sigma} \cdot \boldsymbol{V}) \end{cases} \tag{2.1}$$

$$\frac{\partial}{\partial t} \int_{\Omega} u \, \mathrm{d}\Omega + \int_{S} \mathbf{n} \cdot (u \boldsymbol{V}) \, \mathrm{d}S = \dot{\phi} \tag{2.2}$$

数学公式常用命令请见 WiKibook Mathematics。artracom.sty 中对一些常用数据类型如矢量矩阵等进行了封装，这样的好处是如有一天需要修改矢量的显示形式，只需单独修改 artracom.sty 中的矢量定义即可实现全文档的修改。

2.3.2 表格

请见表 2.1。制表的更多范例，请见 WiKibook Tables。

2.3.3 图片插入

论文中图片的插入通常分为单图和多图，下面分别加以介绍：

表 2.1 这是一个样表。

Table 2.1 This is a sample table.

Row number	This is a multicolumn						
Row 1	1	2	4	5	6	7	8
Row 2	1	2	4	5	6	7	8
Row 3	1	2	4	5	6	7	8
Row 4	1	2	4	5	6	7	8

单图插入：假设插入名为`tc_q_criteria`（后缀可以为.jpg、.png、.pdf，下同）的图片，其效果如图2.1。

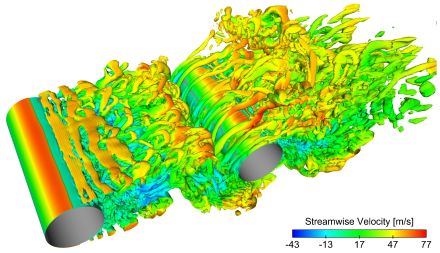

图 2.1 Q 判据等值面图，同时测试一下一个很长的标题，比如这真的是一个很长很长很长很长很长很长很长很长的标题。

Figure 2.1 Isocontour of Q criteria, at the same time, this is to test a long title, for instance, this is a really very long very long very long very long very long title.

如果插图的空白区域过大，以图片`shock_cyn` 为例，自动裁剪如图2.2。

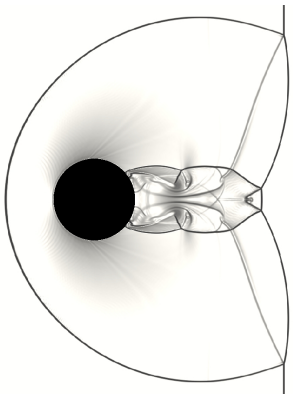

图 2.2 激波圆柱作用。

Figure 2.2 Shock-cylinder interaction.

多图的插入如图2.3，多图不应在子图中给文本子标题，只要给序号，并在主标题中进行引用说明。

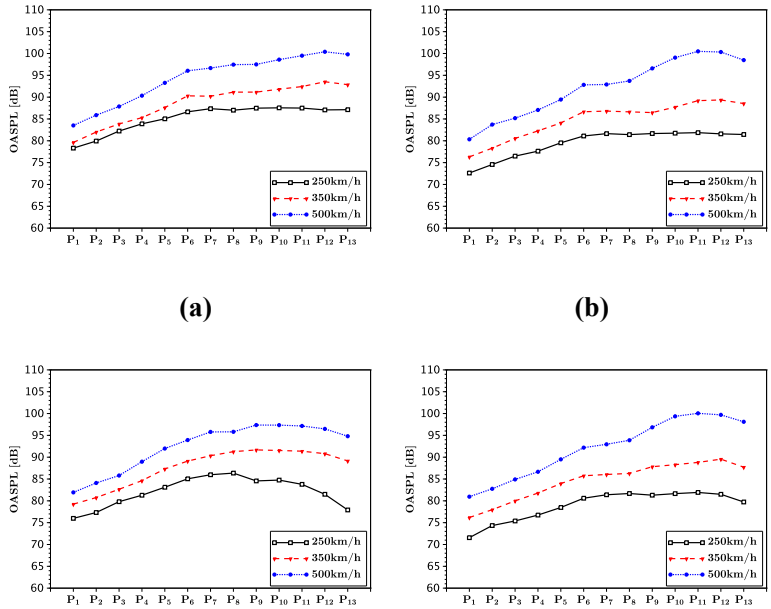

图 2.3 总声压级。(a) 这是子图说明信息，(b) 这是子图说明信息，(c) 这是子图说明信息，(d) 这是子图说明信息。

Figure 2.3 OASPL.(a) This is the explanation of subfig, (b) This is the explanation of subfig, (c) This is the explanation of subfig, (d) This is the explanation of subfig.

2.3.4 算法

如见算法 1，详细使用方法请参见文档 algorithmicx。

Algorithm 1 Euclid's algorithm

```
1: procedure Euclid(a, b)                          ▷ The g.c.d. of a and b
2:     r ← a mod b
3:     while r ≠ 0 do                              ▷ We have the answer if r is 0
4:         a ← b
5:         b ← r
6:         r ← a mod b
7:     end while
8:     return b                                    ▷ The gcd is b
9: end procedure
```

2.3.5 参考文献引用

参考文献引用过程以实例进行介绍，假设需要引用名为"Document Preparation System" 的文献，步骤如下：

1）使用 Google Scholar 搜索 Document Preparation System，在目标条目下点击 Cite，展开后选择 Import into BibTeX 打开此文章的 BibTeX 索引信息，将它们 copy 添加到 ref.bib 文件中（此文件位于 Biblio 文件夹下）。

2）索引第一行 `@article{lamport1986document`，中 `lamport1986document` 即为此文献的 label (**中文文献也必须使用英文 label**，一般遵照：姓氏拼音 + 年份 + 标题第一字拼音的格式)，想要在论文中索引此文献，有两种索引类型：

文本类型：`\citet{lamport1986document}`。正如此处所示 Lamport (1986);

括号类型：`\citep{lamport1986document}`。正如此处所示 (Lamport, 1986)。

多文献索引用英文逗号隔开：

`\citep{lamport1986document, chu2004tushu, chen2005zhulu}`。正如此处所示 (Lamport, 1986; 初景利, 2004; 陈浩元, 2005)

更多例子如：

Walls et al. (2013) 根据... 的研究，首次提出...。其中关于...(Walls et al., 2013)，是当前中国... 得到迅速发展的研究领域 (陈晋镳 等, 1980)。引用同一著者在同一年份出版的多篇文献时, 在出版年份之后用英文小写字母区别，如：(袁训来 等, 2012a,b,c)。同一处引用多篇文献时, 按出版年份由近及远依次标注, 中间用分号

分开。例如 (陈晋镳 等, 1980; Stamerjohanns et al., 2009; 哈里森 · 沃尔德伦, 2012; 牛志明 等, 2013)。

使用著者-出版年制（authoryear）式参考文献样式时，中文文献必须在 BibTeX 索引信息的 **key** 域（请参考 ref.bib 文件）填写作者姓名的拼音，才能使得文献列表按照拼音排序。参考文献表中的条目（不排序号），先按语种分类排列，语种顺序是：中文、日文、英文、俄文、其他文种。然后，中文按汉语拼音字母顺序排列，日文按第一著者的姓氏笔画排序，西文和俄文按第一著者姓氏首字母顺序排列。如中 (牛志明 等, 2013)、日 (ボハンデ, 1928)、英 (Stamerjohanns et al., 2009)、俄 (ДубровинА. И, 1906)。

如此，即完成了文献的索引，请查看下本文档的参考文献一章，看看是不是就是这么简单呢？是的，就是这么简单！

不同文献样式和引用样式，如著者-出版年制（authoryear）、顺序编码制（numbers）、上标顺序编码制（super）可在 Thesis.tex 中对 artratex.sty 调用实现，如：

- `\usepackage[numbers]{artratex}` % 文本: Jones [1]; 括号: [1]
- `\usepackage[super]{artratex}` % 文本: Jones 上标 [1]; 括号: 上标 [1]
- `\usepackage[authoryear]{artratex}` % 文本: Jones (1995); 括号: (Jones, 1995)
- `\usepackage[alpha]{artratex}` % 文本: 不可用; 括号: [Jon95]

当前文档的默认参考文献样式为 **authoryear**。若在上标（**super**）模式下，希望在特定位置将上标改为嵌入式标，可使用

文本类型：`\citetns{lamport1986document,chen2005zhulu}`。

正如此处所示Lamport [1986]; 陈浩元 [2005]

括号类型：`\citepns{lamport1986document,chen2005zhulu}`。

正如此处所示 [Lamport, 1986; 陈浩元, 2005]

参考文献索引更为详细的信息，请见 zepinglee 和 WiKibook Bibliography。

2.4 常见使用问题

1. 模板每次发布前，都已在 Windows，Linux，MacOS 系统上测试通过。下载模板后，若编译出现错误，则请见 ucasthesis 和 LaTeX 知识小站 的 编译指南。

2. 模板文档的编码为 UTF-8 编码。所有文件都必须采用 UTF-8 编码，否则编译后生成的文档将出现乱码文本。若出现文本编辑器无法打开文档或打开文档乱码的问题，请检查编辑器对 UTF-8 编码的支持。如果使用 WinEdt 作为文本

编辑器（**不推荐使用**），应在其 Options -> Preferences -> wrapping 选项卡下将两种 Wrapping Modes 中的内容：

TeX;HTML;ANSI;ASCII|DTX...

修改为：TeX;**UTF-8|ACP;**HTML;ANSI;ASCII|DTX...

同时，取消 Options -> Preferences -> Unicode 中的 Enable ANSI Format。

3. 推荐选择 xelatex 或 lualatex 编译引擎编译中文文档。编译脚本的默认设定为 xelatex 编译引擎。你也可以选择不使用脚本编译，如直接使用 LaTeX 文本编辑器编译。注：LaTeX 文本编辑器编译的默认设定为 pdflatex 编译引擎，若选择 xelatex 或 lualatex 编译引擎，请进入下拉菜单选择。为正确生成引用链接，需要进行全编译。

4. Texmaker 使用简介

(a) 使用 Texmaker“打开 (Open)”Thesis.tex。

(b) 菜单“选项 (Options)”-> “设置当前文档为主文档 (Define as Master Document)”

(c) 菜单“自定义 (User)”-> “自定义命令 (User Commands)”-> “编辑自定义命令 (Edit User Commands)” -> 左侧选择“command 1”，右侧“菜单项 (Menu Item)”填入 Auto Build -> 点击下方“向导 (Wizard)”-> “添加 (Add)”: xelatex + bibtex + xelatex + xelatex + pdf viewer -> 点击“完成 (OK)”

(d) 使用 Auto Build 编译带有未生成引用链接的源文件，可以仅使用 xelatex 编译带有已经正确生成引用链接的源文件。

(e) 编译完成，“查看 (View)”PDF，在 PDF 中“ctrl+click”可链接到相对应的源文件。

5. 模版的设计可能地考虑了适应性。致谢等所有条目都是通过最为通用的 `\chapter{item name}` and `\section*{item name}` 来显式实现的 (请观察 Backmatter.tex)，从而可以随意添加，放置，和修改，如同一般章节。对于图表目录名称则可在 ucasthesis.cfg 中进行修改。

6. 设置文档样式: 在 artratex.sty 中搜索关键字定位相应命令，然后修改

(a) 正文行距：启用和设置 `\linespread{1.5}`，默认 1.5 倍行距。

(b) 参考文献行距：修改 `\setlength{\bibsep}{0.0ex}`

(c) 目录显示级数：修改 `\setcounter{tocdepth}{2}`

(d) 文档超链接的颜色及其显示：修改 `\hypersetup`

7. 文档内字体切换方法：

- 宋体：国科大论文模板 ucasthesis 或 国科大论文模板 ucasthesis
- 粗宋体：**国科大论文模板 ucasthesis** 或 **国科大论文模板 ucasthesis**
- 黑体：国科大论文模板 ucasthesis 或 国科大论文模板 ucasthesis
- 粗黑体：**国科大论文模板 ucasthesis** 或 **国科大论文模板 ucasthesis**
- 仿宋：国科大论文模板 `ucasthesis` 或 国科大论文模板 `ucasthesis`

- 粗仿宋：国科大论文模板 **ucasthesis** 或 国科大论文模板 **ucasthesis**
- 楷体：国科大论文模板 *ucasthesis* 或 国科大论文模板 *ucasthesis*
- 粗楷体：**国科大论文模板 *ucasthesis*** 或 **国科大论文模板 *ucasthesis***

8. 封面下划线上的文本不居中下划线，这是因为下划线前面还有字头，导致文本只能在页面居中和在下划线上居中二选一。当前封面采取页面居中。如需要调整文本在下划线上的位置，可用 `\hspace{+/- n.0em}` 命令来插入或删除 n 个空格，进行手动调整，比如

```
\advisor{\hspace{+3.0em} xxx~研究员~xxx单位}
```

有时下划线看上去粗细不一致，这是显示的问题，打印正常。

附录 A　中国科学院大学学位论文撰写要求

学位论文是研究生科研工作成果的集中体现，是评判学位申请者学术水平、授予其学位的主要依据，是科研领域重要的文献资料。根据《科学技术报告、学位论文和学术论文的编写格式》（GB/T 7713-1987）、《学位论文编写规则》（GB/T 7713.1-2006）和《文后参考文献著录规则》（GB7714—87）等国家有关标准，结合中国科学院大学（以下简称“国科大”）的实际情况，特制订本规定。

A.1　论文无附录者无需附录部分

A.2　测试公式编号

$$\begin{cases} \frac{\partial \rho}{\partial t} + \nabla \cdot (\rho \boldsymbol{V}) = 0 \text{ times font test} \\ \frac{\partial (\rho \boldsymbol{V})}{\partial t} + \nabla \cdot (\rho \boldsymbol{V} \boldsymbol{V}) = \nabla \cdot \boldsymbol{\sigma} \text{ times font test} \\ \frac{\partial (\rho E)}{\partial t} + \nabla \cdot (\rho E \boldsymbol{V}) = \nabla \cdot (k \nabla T) + \nabla \cdot (\boldsymbol{\sigma} \cdot \boldsymbol{V}) \end{cases} \tag{A.1}$$

$$\frac{\partial}{\partial t} \int\limits_{\Omega} u \, \mathrm{d}\Omega + \int\limits_{S} \mathbf{n} \cdot (u \boldsymbol{V}) \, \mathrm{d}S = \dot{\phi} \tag{A.2}$$

A.3　测试生僻字

霜蟾盥薇曜灵霜颸妙鬘虚霩淩澌菀枯菡萏泬寥窅冥稖褪濩落雲雲便嬛岧峣瀺灂姽婳愔嫕飒纚棽俪緌冤莩甲摛藻卮言倥侗椒觞期颐夜阑彬蔚倥偬澄廓簪缨陟遐迤逦缥缃鹣鲽憯懔闺闼璀错媕婀噌吰澒洞阛阓覼缕玓瓅逡巡諓諓琭琭瀌瀌踽踽叆叇氤氲瓠犀流眄蹀躞赟嬛茕頔璎珞螓首蘅皋惏悷缱绻昶皴皱颟顸愀然菡萏卑陬纯懿犇麤掱喤墟堑墎壄墐墒墒墓墔墕墖墘墖墚墛坠墝增墠墡墢墣墤墥墦墧墨墩墪樽墬墭堕墯墰墱墲坟墴墵垯墷墸墹墺墙墼墽垦墿壀壁壂壃壄壅壆坛壈壉壊垱壌壍埙壏壐壑壒压壔壕壖壗垒圹垆壛壜壝垄壠壡坜壣壤壥壦壧壨坝壪圭嫶嫷嫸嫹嫺娴嫼嫽嫾婳妫嬁嬂嬃嬄嬅嬆嬇娆嬉嬊娇嬍嬎嬏嬐嬑嬒嬓嬔嬕嬖嬗嬘嫱嬚嬛嬜嬞嬟嬠嫒嬢嬣嬥嬦嬧嬨嬩嫔嬫嬬奶嬬嬮嬯婴嬱嬲嬳嬴嬵嬶嬷婶嬹嬺嬻嬼嬽嬾嬿孁孂娘孄孅孆孇孆孈孉孊娈孋孊孍孎孏嫫婿媚嵭嵮嵯嵰嵱嵲嵳嵴嵵嵶嵷嵸嵹嵺嵻嵼嵽嵾嵿嶀嵝嶂崭嶅嶆岖嶈嶉嶊嶋嶌嶍嶎嶏嶐嶑嶒嶓嵚嶕嶖嶘嶙嶚嶛嶜嶝嶞嶟峤嶡峣嶣嶤嶥嶦峄峃嶩嶪嶫嶬嶭崄嶯嶰嶱嶲嶳岙嶵嶶嶷嶸嶹岭

巀屿岳岎巆巁巂巃巄巅巇巈巊巋巌巎巏巐巑巒巓巔巕巖巗巘巙巚帋帎帒帓帟帣帤帨帩帪帬帯帰帱帴帹帺帻帽帾幀幁幃幆幇幈幉幊幋幍幎幏幐幑幒幓幖幙幚幜幝幟幠幣幤幥幦幧幨幩幪幫幬幭幮幯幰庁庈庘庛庝庢庣庤庨庩庪庮庯庰庱庲庴庺庻庼庽庿廀廁廂廃廄廅廆廇廈廋廌廍廎廏廐廔廕廗廘廙廚廜廝廞廟廠廡廢廣廤廥廦廧廩廫廬廭廮廯廰廱廲巡廸廹廻廼廽廿弁弅弆弇弉弖弙弚弜弝弞弡弢弣弤弨弩弪弫弬弭弮弰弲弳弴弶弸弻弼弽弿彀彁彂彃彄彅彆彇彋彍彑彛彜彞彟彠彶彾彿徂徃徆徎徏徔径徚徛徜徝從徟徠徢徣徤徥徦徧徨復循徫徬徯徰徱徲徳徴徵徶德徸徹徺徻徿忀忂忄忈忉忊忋忎忓忔忕忚忛応忝忞忟忡忣忦忨忩忬忯忰忱忲忳忴忶忷忹忺忼怇怈怉怋怌怐怑怓怗怘怚怞怟怢怣怤怬怭怮怰怱怲怳怴怶怷怸怹怺怾怿恀恄恅恇恈恊恌恎恏恑恓恔恖恗恘恛恜恞恟恠恡恥恦恮恱恲恴恵恷恾悀悁悂悆悇悈悊悋悎悏悐悑悓悕悗悘悙悜悞悡悢悤悥悧悩悪悮悰悳悵悶悷悹悺悽悾惂惃惄惇惈惉惌惍惎惏惐惒惓惔惖惗惙惛惞惡惢惣惤惥惪惱惲惵惷惸惻惼惽惾惿愂愃愄愅愇愊愋愌愐愑愒愓愔愖愗愘愙愛愜愝愞愡愢愥愨愩愪愬愭愮愯愰愱愲愳愴愵愶愷愸愹愺愻愼愽愾慀慁慂慃栁慅慆慇慉態慍慏慐慒慓慔慖慗慘慙慚慛慜慞慟慠慡慣慤慥慦慩慪慫慬慭慮慯慱慲慳慴慶慸慹慺慻慼慽慾慿憀憁憂憃憄憅憆憇憈憉憊憌憍憏憐憑憒憓憕憖憗憘憙憚憛憜憞憟憠憡憢憣憤憥憦憪憫憭憮憯憰憱憳憴憵憶憸憹憺憻憼憽憿懀懁懃懄懅懆懇應懌懍懎懏懐懓懕懖懗懘懙懚懛懜懝懞懟懠懡懢懤懥懧懨懩懪懫懬懭懮懯懰懱懲懳懴懶懷懸懹懺懻懼懽懾戀戁戂戃戄戅戇戉戓戔戙戜戝戞戠戣戦戧戨戩戫戭戯戰戱戲戵戶戸戹戺戻戼扂扄扅扆扊

参考文献

陈浩元. 2005. 著录文后参考文献的规则及注意事项[J]. 编辑学报, 17(6): 413-415.

陈晋镳, 张惠民, 朱士兴, 等. 1980. 蓟县震旦亚界研究[M]//中国地质科学院天津地质矿产研究所. 中国震旦亚界. 天津: 天津科学技术出版社: 56-114.

初景利. 2004. 图书馆数字参考咨询服务研究[M]. 北京: 北京图书馆出版社.

哈里森·沃尔德伦. 2012. 经济数学与金融数学[M]. 谢远涛, 译. 北京: 中国人民大学出版社: 235-236.

牛志明, 斯温兰德, 雷光春. 2013. 综合湿地管理国际研讨会论文集[C]. 北京: 海洋出版社.

袁训来, 陈哲, 肖书海. 2012a. 蓝田生物群: 一个认识多细胞生物起源和早期演化的新窗口 – 篇一[J]. 科学通报, 57(34): 3219.

袁训来, 陈哲, 肖书海. 2012b. 蓝田生物群: 一个认识多细胞生物起源和早期演化的新窗口 – 篇二[J]. 科学通报, 57(34): 3219.

袁训来, 陈哲, 肖书海. 2012c. 蓝田生物群: 一个认识多细胞生物起源和早期演化的新窗口 – 篇三[J]. 科学通报, 57(34): 3219.

邵健雄. 2016. 下一代可信计算协议的设计与分析[D]. 中国科学院大学.

ボハンデ. 1928. 過去及び現在に於ける英国と会[J]. 日本時報, 17: 5-9.

ABADI M. 1999. Secrecy by typing in security protocols[J]. Journal of the ACM (JACM), 46(5): 749-786.

ABADI M, BLANCHET B. 2002. Analyzing security protocols with secrecy types and logic programs[J]. ACM SIGPLAN Notices, 37(1): 33-44.

ABADI M, BLANCHET B. 2005. Analyzing security protocols with secrecy types and logic programs[J]. Journal of the ACM (JACM), 52(1): 102-146.

ABADI M, FOURNET C. 2001. Mobile values, new names, and secure communication[C]//ACM Sigplan Notices: volume 36. ACM: 104-115.

ABADI M, GORDON A D. 1997. A calculus for cryptographic protocols: The spi calculus[C]// Proceedings of the 4th ACM conference on Computer and communications security. ACM: 36-47.

ABADI M, ROGAWAY P. 2000. Reconciling two views of cryptography[C]//Proceedings of the IFIP International Conference on Theoretical Computer Science. Springer: 3-22.

ABADI M, BLANCHET B, FOURNET C. 2017. The applied pi calculus: mobile values, new names, and secure communication[J]. Journal of the ACM (JACM), 65(1): 1.

ADIDA B. 2008. Helios: Web-based open-audit voting.[C]//USENIX security symposium: volume 17. 335-348.

ARAPINIS M, RITTER E, RYAN M D. 2011. Statverif: Verification of stateful processes[C]//2011 24th Computer Security Foundations Symposium. IEEE: 33-47.

ARAPINIS M, LIU J, RITTER E, et al. 2014. Stateful applied pi calculus[C]//International Conference on Principles of Security and Trust. Springer: 22-41.

AU M H, KAPADIA A. 2012a. Perm: Practical reputation-based blacklisting without ttps[C]// Proceedings of the 2012 ACM conference on Computer and communications security. ACM: 929-940.

AU M H, KAPADIA A, SUSILO W. 2012b. Blacr: Ttp-free blacklistable anonymous credentials with reputation[Z].

BACKES M, PFITZMANN B, WAIDNER M. 2003. A composable cryptographic library with nested operations[C]//Proceedings of the 10th ACM conference on Computer and communications security. ACM: 220-230.

BACKES M, MAFFEI M, UNRUH D. 2008. Zero-knowledge in the applied pi-calculus and automated verification of the direct anonymous attestation protocol[C]//Security and Privacy, 2008. SP 2008. IEEE Symposium on. IEEE: 202-215.

BACKES M, HOFHEINZ D, UNRUH D. 2009. Cosp: A general framework for computational soundness proofs[C]//Proceedings of the 16th ACM conference on Computer and communications security. ACM: 66-78.

BACKES M, MAFFEI M, UNRUH D. 2010. Computationally sound verification of source code [C]//Proceedings of the 17th ACM conference on Computer and communications security. ACM: 387-398.

BACKES M, MOHAMMADI E, RUFFING T. 2014. Computational soundness results for proverif [C]//International Conference on Principles of Security and Trust. Springer: 42-62.

BALDIMTSI F, LYSYANSKAYA A. 2013a. Anonymous credentials light[C]//Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security. ACM: 1087-1098.

BALDIMTSI F, LYSYANSKAYA A. 2013b. On the security of one-witness blind signature schemes [C]//International Conference on the Theory and Application of Cryptology and Information Security. Springer: 82-99.

BARTHE G, GRÉGOIRE B, ZANELLA BÉGUELIN S. 2009. Formal certification of code-based cryptographic proofs[J]. ACM SIGPLAN Notices, 44(1): 90-101.

BARTHE G, GRÉGOIRE B, HERAUD S, et al. 2011. Computer-aided security proofs for the working cryptographer[C]//Annual Cryptology Conference. Springer: 71-90.

BELLARE M, ROGAWAY P. 2006. The security of triple encryption and a framework for code-based game-playing proofs[C]//Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer: 409-426.

BHARGAVAN K, BLANCHET B, KOBEISSI N. 2017. Verified models and reference implementations for the tls 1.3 standard candidate[C]//Security and Privacy (SP), 2017 IEEE Symposium on. IEEE: 483-502.

BLANCHET B. 2006. A computationally sound mechanized prover for security protocols[C]// Security and Privacy, 2006 IEEE Symposium on. IEEE: 15-pp.

BLANCHET B. 2001. An efficient cryptographic protocol verifier based on prolog rules[C]//csfw. IEEE: 0082.

BLANCHET B. 2002. From secrecy to authenticity in security protocols[C]//International Static Analysis Symposium. Springer: 342-359.

BLANCHET B. 2004. Automatic proof of strong secrecy for security protocols[M]. IEEE.

BLANCHET B. 2007. Computationally sound mechanized proofs of correspondence assertions[C]// Computer Security Foundations Symposium, 2007. CSF'07. 20th IEEE. IEEE: 97-111.

BLANCHET B. 2008. A computationally sound mechanized prover for security protocols[J]. IEEE Transactions on Dependable and Secure Computing, 5(4): 193-207.

BLANCHET B. 2009. Automatic verification of correspondences for security protocols[J]. Journal of Computer Security, 17(4): 363-434.

BLANCHET B. 2017. Symbolic and computational mechanized verification of the arinc823 avionic protocols[C]//Computer Security Foundations Symposium (CSF), 2017 IEEE 30th. IEEE: 68-82.

BLANCHET B. 2018. Composition theorems for CryptoVerif and application to TLS 1.3[C]// Computer Security Foundations Symposium (CSF), 2017 IEEE 31th. Oxford, UK: IEEE Computer Society.

BLANCHET B, CHAUDHURI A. 2008a. Automated formal analysis of a protocol for secure file sharing on untrusted storage[C]//Security and Privacy, 2008. SP 2008. IEEE Symposium on. IEEE: 417-431.

BLANCHET B, SMYTH B. 2016. Automated reasoning for equivalences in the applied pi calculus with barriers[C]//Computer Security Foundations Symposium (CSF), 2016 IEEE 29th. IEEE: 310-324.

BLANCHET B, ABADI M, FOURNET C. 2005. Automated verification of selected equivalences for security protocols[C]//Logic in Computer Science, 2005. LICS 2005. Proceedings. 20th Annual IEEE Symposium on. IEEE: 331-340.

BLANCHET B, JAGGARD A D, SCEDROV A, et al. 2008b. Computationally sound mechanized proofs for basic and public-key kerberos[C]//Proceedings of the 2008 ACM symposium on Information, computer and communications security. ACM: 87-99.

BRANDS S. 2000. Rethinking public key infrastructures and digital certificates: building in privacy [M]. Mit Press.

BRICKELL E, LI J. 2007. Enhanced privacy id: A direct anonymous attestation scheme with enhanced revocation capabilities[C]//Proceedings of the 2007 ACM workshop on Privacy in electronic society. ACM: 21-30.

BRICKELL E, LI J. 2010. A pairing-based daa scheme further reducing tpm resources[C]// International Conference on Trust and Trustworthy Computing. Springer: 181-195.

BRICKELL E, CAMENISCH J, CHEN L. 2004. Direct anonymous attestation[C]//Proceedings of the 11th ACM conference on Computer and communications security. ACM: 132-145.

BRICKELL E, CHEN L, LI J. 2008. A new direct anonymous attestation scheme from bilinear maps[C]//International Conference on Trusted Computing. Springer: 166-178.

BRICKELL E, CHEN L, LI J. 2009. Simplified security notions of direct anonymous attestation and a concrete scheme from pairings[J]. International journal of information security, 8(5): 315-330.

BRICKELL E, CHEN L, LI J. 2012. A static diffie-hellman attack on several direct anonymous attestation schemes[C]//International Conference on Trusted Systems. 95-111.

BRUSCHI D, CAVALLARO L, LANZI A, et al. 2005. Replay attack in tcg specification and solution [C]//Computer Security Applications Conference, 21st Annual. IEEE: 11-pp.

BURROWS M, ABADI M, NEEDHAM R M. 1989. A logic of authentication[J]. Proc. R. Soc. Lond. A, 426(1871): 233-271.

CACHIN C, CHANDRAN N. 2009. A secure cryptographic token interface[C]//IEEE Computer Security Foundations Symposium. 141-153.

CADÉ D, BLANCHET B. 2013. From computationally-proved protocol specifications to implementations and application to ssh[J]. JoWUA, 4(1): 4-31.

CAMENISCH J, LYSYANSKAYA A. 2001. An efficient system for non-transferable anonymous credentials with optional anonymity revocation[C]//International Conference on the Theory and Applications of Cryptographic Techniques. Springer: 93-118.

CAMENISCH J, LYSYANSKAYA A. 2002. A signature scheme with efficient protocols[M]// Security in communication networks. Springer: 268-289.

CAMENISCH J, LYSYANSKAYA A. 2004. Signature schemes and anonymous credentials from bilinear maps[C]//Annual International Cryptology Conference. Springer: 56-72.

CAMENISCH J, DRIJVERS M, LEHMANN A. 2016. Universally composable direct anonymous attestation[C]//Proceedings, Part II, of the 19th IACR International Conference on Public-Key Cryptography — PKC 2016 - Volume 9615. 234-264.

CAMENISCH J, et al. 2010. Specification of the identity mixer cryptographic library[R]. Tech. rep.

CANETTI R, HERZOG J. 2006. Universally composable symbolic analysis of mutual authentication and key-exchange protocols[C]//Theory of Cryptography Conference. Springer: 380-403.

CHASE M, MEIKLEJOHN S, ZAVERUCHA G. 2014. Algebraic macs and keyed-verification anonymous credentials[C]//Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. ACM: 1205-1216.

CHAUM D. 1985. Security without identification: Transaction systems to make big brother obsolete [J]. Communications of the ACM, 28(10): 1030-1044.

CHAUM D, FIAT A, NAOR M. 1988. Untraceable electronic cash[C]//Conference on the Theory and Application of Cryptography. Springer: 319-327.

CHEN L, LI J. 2013. Flexible and scalable digital signatures in tpm 2.0[C]//Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security. ACM: 37-48.

CHEN L, RYAN M. 2009a. Attack, solution and verification for shared authorisation data in tcg tpm[C]//International Workshop on Formal Aspects in Security and Trust. Springer: 201-216.

CHEN L, RYAN M. 2009b. Offline dictionary attack on tcg tpm weak authorisation data, and solution[M]//Future of Trust in Computing. Springer: 193-196.

CHEN L, MORRISSEY P, SMART N P. 2009c. Daa: Fixing the pairing based protocols.[J]. IACR Cryptology ePrint Archive, 2009: 198.

CHEN L, PAGE D, SMART N P. 2010. On the design and implementation of an efficient daa scheme [C]//International Conference on Smart Card Research and Advanced Applications. Springer: 223-237.

CHEVAL V, BLANCHET B. 2013. Proving more observational equivalences with proverif[C]// International Conference on Principles of Security and Trust. Springer: 226-246.

CHOTHIA T, SMYTH B, STAITE C. 2015. Automatically checking commitment protocols in proverif without false attacks[C]//International Conference on Principles of Security and Trust. Springer: 137-155.

CHU X, FENG D. 2015. On the provable security of TPM2.0 cryptography apis[J]. IJES, 7(3/4): 230-243.

CLARKSON M R, CHONG S, MYERS A C. 2008. Civitas: Toward a secure voting system[C]// Security and Privacy, 2008. SP 2008. IEEE Symposium on. IEEE: 354-368.

CORTIER V, WARINSCHI B. 2005. Computationally sound, automated proofs for security protocols[C]//European Symposium on Programming. Springer: 157-171.

CORTIER V, STEEL G. 2009. A generic security api for symmetric key management on cryptographic devices[C]//European Symposium on Research in Computer Security. 605-620.

CORTIER V, STEEL G. 2014. A generic security api for symmetric key management on cryptographic devices[J]. Information & Computation, 238(C): 208-232.

DATTA A, FRANKLIN J, GARG D, et al. 2009. A logic of secure systems and its application to trusted computing[C]//Security and Privacy, 2009 30th IEEE Symposium on. IEEE: 221-236.

DAUBIGNARD M, LUBICZ D, STEEL G. 2014. A secure key management interface with asymmetric cryptography[C]//International Conference on Principles of Security and Trust. 63-82.

DELAUNE S, KREMER S, RYAN M D, et al. 2010. A formal analysis of authentication in the tpm [C]//International Workshop on Formal Aspects in Security and Trust. Springer: 111-125.

DELAUNE S, KREMER S, RYAN M D, et al. 2011. Formal analysis of protocols based on tpm state registers[C]//24th IEEE Computer Security Foundations Symposium (CSF 2011). IEEE: 66-80.

DOLEV D, YAO A. 1981. On the security of public key protocols[C]//Foundations of Computer Science, 1981. SFCS'81. 22nd Annual Symposium on. IEEE: 350-357.

DOLEV D, EVEN S, KARP R M. 1983. On the security of ping-pong protocols[C]//Advances in Cryptology. Springer: 177-186.

DUTERTRE B, SCHNEIDER S. 1997. Using a pvs embedding of csp to verify authentication protocols[C]//International Conference on Theorem Proving in Higher Order Logics. Springer: 121-136.

FÁBREGA F J T, HERZOG J C, GUTTMAN J D. 1998. Strand spaces: Why is a security protocol correct?[C]//Security and Privacy, 1998. Proceedings. 1998 IEEE Symposium on. IEEE: 160-171.

GORDON A D, JEFFREY A. 2003. Authenticity by typing for security protocols 1[J]. Journal of computer security, 11(4): 451-519.

GÜRGENS S, RUDOLPH C, SCHEUERMANN D, et al. 2007. Security evaluation of scenarios based on the tcg's tpm specification[C]//European Symposium on Research in Computer Security. Springer: 438-453.

HALEVI S. 2005. A plausible approach to computer-aided cryptographic proofs.[J]. IACR Cryptology ePrint Archive, 2005: 181.

HENRY R, GOLDBERG I. 2013. Thinking inside the blac box: smarter protocols for faster anonymous blacklisting[C]//Proceedings of the 12th ACM workshop on Workshop on privacy in the electronic society. ACM: 71-82.

ISO/IEC 11889. 2009. Pas dis 11889: Information technology - security techniques - trusted platform module[EB/OL]. ISO/IEC. http://www.iso.org/iso/catalogue_detail.htm?csnumber=50970.

ISO/IEC 11889. 2015. Pas dis 11889: Information technology - security techniques - trusted platform module[EB/OL]. ISO/IEC. https://www.iso.org/standard/66510.html.

JANVIER R, LAKHNECH Y, MAZARÉ L. 2005. Completing the picture: Soundness of formal encryption in the presence of active adversaries[C]//European Symposium on Programming. Springer: 172-185.

KEMMERER R, MEADOWS C, MILLEN J. 1994. Three systems for cryptographic protocol analysis[J]. Journal of CRYPTOLOGY, 7(2): 79-130.

KREMER S, KÜNNEMANN R. 2016. Automated analysis of security protocols with global state [J]. Journal of Computer Security, 24(5): 583-616.

LAMPORT L. 1986. Document preparation system[M]. Addison-Wesley Reading, MA.

LIN A H. 2005. Automated analysis of security apis[D]. Massachusetts Institute of Technology.

LOFGREN P, HOPPER N. 2011. Faust: Efficient, ttp-free abuse prevention by anonymous whitelisting[C]//Proceedings of the 10th annual ACM workshop on Privacy in the electronic society. ACM: 125-130.

MCCARTHY A, SMYTH B, QUAGLIA E A. 2014. Hawk and aucitas: e-auction schemes from the helios and civitas e-voting schemes[C]//International Conference on Financial Cryptography and Data Security. Springer: 51-63.

MEADOWS C. 1994. A model of computation for the nrl protocol analyzer[C]//Computer Security Foundations Workshop VII, 1994. CSFW 7. Proceedings. IEEE: 84-89.

MICROSOFT. 2017. Trusted Platform Module Technology Overview[EB/OL]. https://technet.microsoft.com/en-us/itpro/windows/keep-secure/trusted-platform-module-overview.

MILLEN J K, CLARK S C, FREEDMAN S B. 1987. The interrogator: Protocol secuity analysis [J]. IEEE Transactions on software Engineering(2): 274-288.

MILNER R. 1999. Communicating and mobile systems: the pi calculus[M]. Cambridge university press.

NAKAMOTO S. 2008. Bitcoin: A peer-to-peer electronic cash system[Z]. Working Paper.

NEEDHAM R M, SCHROEDER M D. 1978. Using encryption for authentication in large networks of computers[J]. Communications of the ACM, 21(12): 993-999.

OWRE S, RUSHBY J M, SHANKAR N. 1992. Pvs: A prototype verification system[C]// International Conference on Automated Deduction. Springer: 748-752.

PAIOLA M, BLANCHET B. 2012. Verification of security protocols with lists: from length one to unbounded length[C]//International Conference on Principles of Security and Trust. Springer: 69-88.

PAQUIN C, ZAVERUCHA G. 2011. U-prove cryptographic specification v1. 1[J]. Technical Report, Microsoft Corporation.

PAULSON L C. 1998. The inductive approach to verifying cryptographic protocols[J]. Journal of computer security, 6(1-2): 85-128.

SCHMIDT B, SASSE R, CREMERS C, et al. 2014. Automated verification of group key agreement protocols[C]//2014 IEEE Symposium on Security and Privacy (SP). IEEE: 179-194.

SHAO J, FENG D, QIN Y. 2013. Type-based analysis of protected storage in the tpm[C]// International Conference on Information and Communications Security. Springer: 135-150.

SHAO J, QIN Y, FENG D. 2016. Computational soundness results for stateful applied pi calculus [C]//International Conference on Principles of Security and Trust. Springer: 254-275.

SHAO J, QIN Y, FENG D. 2018. Formal analysis of hmac authorisation in the tpm2.0 specification [J]. Iet Information Security, 12(2): 133-140.

SMYTH B, RYAN M, CHEN L. 2011. Formal analysis of anonymity in ecc-based direct anonymous attestation schemes[C]//International Workshop on Formal Aspects in Security and Trust. Springer: 245-262.

SMYTH B, RYAN M D, CHEN L. 2015. Formal analysis of privacy in direct anonymous attestation schemes □[J]. Science of Computer Programming, 111: 300-317.

SONG D X, BEREZIN S, PERRIG A. 2001. Athena: a novel approach to efficient automatic security protocol analysis 1[J]. Journal of Computer Security, 9(1-2): 47-74.

STAMERJOHANNS H, GINEV D, DAVID C, et al. 2009. MathML-aware article conversion from LaTeX[J]. Towards a Digital Mathematics Library, 16(2): 109-120.

TCG. 2003. Trusted Platform Module Library Specification, Family “1.2”, Revision 116[EB/OL]. TCG. http://www.trustedcomputinggroup.org/tpm-main-specification.

TCG. 2014. Trusted Platform Module Library Specification, Family “2.0”, Level 00, Revision 01.38 [EB/OL]. TCG. http://www.trustedcomputinggroup.org/tpm-library-specification.

TSANG P P, AU M H, KAPADIA A, et al. 2007. Blacklistable anonymous credentials: blocking misbehaving users without ttps[C]//Proceedings of the 14th ACM conference on Computer and communications security. ACM: 72-81.

TSANG P P, AU M H, KAPADIA A, et al. 2008. Perea: Towards practical ttp-free revocation in anonymous authentication[C]//Proceedings of the 15th ACM conference on Computer and communications security. ACM: 333-344.

WALLS S C, BARICHIVICH W J, BROWN M E. 2013. Drought, deluge and declines: the impact of precipitation extremes on amphibians in a changing climate[J/OL]. Biology, 2(1): 399-418 [2013-11-04]. http://www.mdpi.com/2079-7737/2/1/399. DOI: 10.3390/biology2010399.

WANG W, FENG D, QIN Y, et al. 2014. Exblacr: extending blacr system[C]//Australasian Conference on Information Security and Privacy. Springer: 397-412.

WIKIBOOK. 2014. http://en.wikibooks.org/wiki/latex[M]. On-line Resources.

XI L, FENG D. 2014a. Farb: fast anonymous reputation-based blacklisting without ttps[C]// Proceedings of the 13th Workshop on Privacy in the Electronic Society. ACM: 139-148.

XI L, FENG D. 2014b. Formal analysis of daa-related apis in tpm 2.0[C]//International Conference on Network and System Security. Springer: 421-434.

XI L, SHAO J, YANG K, et al. 2014c. Arbra: anonymous reputation-based revocation with efficient authentication[C]//International Conference on Information Security. Springer: 33-53.

XIAOFENG C, DENGGUO F. 2008. Direct anonymous attestation for next generation tpm[J]. Journal of Computers, 3(12): 43-50.

YANG R, AU M H, XU Q, et al. 2018. Decentralized blacklistable anonymous credentials with reputation[C]//Australasian Conference on Information Security and Privacy. Springer International Publishing: 720-738.

YU K Y, YUEN T H, CHOW S S, et al. 2012. Pe (ar) 2: Privacy-enhanced anonymous authentication with reputation and revocation[C]//European Symposium on Research in Computer Security. Springer: 679-696.

ZHANG Q, ZHAO S, QIN Y, et al. 2014. Formal analysis of tpm2. 0 key management apis[J]. Chinese science bulletin, 59(32): 4210-4224.

ZHAO S, XI L, ZHANG Q, et al. 2015. Security analysis of sm2 key exchange protocol in tpm2. 0 [J]. Security and Communication Networks, 8(3): 383-395.

ДубровинА. И. 1906. Открытое письмо Председателя Главного Совета Союза Русского Народа Санкт-Петербургскому Антонию, Первенствующему члену Священного Синода[J]. Вече: 1-3.

作者简历及攻读学位期间发表的学术论文与研究成果

本科生无需此部分。

作者简历

casthesis 作者

吴凌云，福建省屏南县人，中国科学院数学与系统科学研究院博士研究生。

ucasthesis 作者

莫晃锐，湖南省湘潭县人，中国科学院力学研究所硕士研究生。

已发表 (或正式接受) 的学术论文:

[1] ucasthesis: A LaTeX Thesis Template for the University of Chinese Academy of Sciences, 2014.

申请或已获得的专利:

(无专利时此项不必列出)

参加的研究项目及获奖情况:

可以随意添加新的条目或是结构。

致　谢

感激 casthesis 作者吴凌云学长，gbt7714-bibtex-style 开发者 zepinglee，和 ctex 众多开发者们。若没有他们的辛勤付出和非凡工作，LaTeX 菜鸟的我是无法完成此国科大学位论文 LaTeX 模板 ucasthesis 的。在 LaTeX 中的一点一滴的成长源于开源社区的众多优秀资料和教程，在此对所有 LaTeX 社区的贡献者表示感谢！

ucasthesis 国科大学位论文 LaTeX 模板的最终成型离不开以霍明虹老师和丁云云老师为代表的国科大学位办公室老师们制定的官方指导文件和众多 ucasthesis 用户的热心测试和耐心反馈，在此对他们的认真付出表示感谢。特别对国科大的赵永明同学的众多有效反馈意见和建议表示感谢，对国科大本科部的陆晴老师和本科部学位办的丁云云老师的细致审核和建议表示感谢。谢谢大家的共同努力和支持，让 ucasthesis 为国科大学子使用 LaTeX 撰写学位论文提供便利和高效这一目标成为可能。