实验室代码：2002DP173012

2017 年度报告

实验室名称：中国科学院数学机械化重点实验室
归口领域：数理
依托单位:中国科学院数学与系统科学研究院
实验室主任：李洪波
联系人:周代珍、李佳
联系电话：82541809
填报时间：2018.3.22

目录

第一部分 实验室基本情况

实验室中文名称	中国科学院数学机械化重点实验室		
实验室英文名称	Key Laboratory of Mathematics Mechanization (KLMM) , CAS		
实验室代码	2002DP173012		
实验室类型	中科院重点实验室		
依托单位	中国科学院数学与系统科学研究院		
实验室主任	李洪波		
学术委员会主任	李邦河		
实验室通讯地址	北京海淀区中关村东路 55 号		
邮政编码	100190		
联系人	周代珍、李佳		
联系电话	82541851		
传真	82541809		
电子邮箱	dzhou@mmrc.iss.ac.cn； jiali@mmrc.iss.ac.cn		
实验室网址	http://mmrc.amss.cas.cn/		
研究性质	应用基础研究		
归口领域	数理		
	学科 1	学科 2	学科 3
硕士点	基础数学	应用数学	计算机科学与技术
博士点	基础数学	应用数学	计算机科学与技术
博士后流动站	基础数学	应用数学	

实验室类型：国家研究中心、国家重点实验室、中科院重点实验室。
研究性质：基础研究、应用基础研究、社会公益性研究、高技术研发。
归口领域：化学、数理、地学、生命（生物、医学）、信息、材料、工程。

定位
数学机械化重点实验室的战略目标是**引领数学机械化研究，发展数学机械化理论与高效算法，**为科学研究与高技术研究中的脑力劳动的机械化提供有力工具，为提高我国知识与技术创新的效率做出实质性贡献。 实验室应用数学机械化方法**解决信息安全、数控技术、机器人、计算机辅助设计(CAD)等高科技领域的关键问题，开发基于数学机械化方法的智能软件，**为我国相关高技术领域的技术创新创造条件。 实验室是**凝聚和培养相关学科具有重要国际影响的杰出人才，进行数学机械化方面高层次国际学术交流的中心**。

序号	研究方向	研究内容	对应研究所一三五

1	数学机械化理论	符号计算、计算代数几何、计算几何、计算拓扑、计算群论、符号分析、自动推理、混合计算、非线性数学物理方程、数学机械化方法的高技术应用、智能软件开发	突破二，培育五
2	信息安全的数学理论	有限域理论、密码分析、安全多方计算理论、抗量子算法攻击分析	突破二，培育五
参与四类机构情况			
1	数学科学卓越创新中心		

研究内容：为各研究方向的详细说明。

参与四类机构情况：填写参与研究所的四类机构建设情况。如果有参与，请填写研究所的四类机构类型；如果未参与，填写否。

第二部分 年度总结

一、研究水平与贡献

1. 承担任务

（全面概述实验室一年来承担科研任务的总体情况,取得的研究成果,包括奖励、论文、专著、授权发明专利等，以及实验室在本学科领域 1 区发表的论文占总论文数的比例等。）

本年度实验室总计承担了 34 个科研项目，其中承担科技委项目 1 项，参加国家重点研发计划课题 1 项，参加 863 计划子课题 1 项，主持国家自然科学基金 10 项，主持省部级项目 15 项，主持其他横向课题 6 项。实验室在数学机械化的主要方向，包括符号计算、信息安全、在其他学科中的应用，取得一系列成果，共获得 9 项奖励，发表和接收论文 57 篇，出版专著 2 部，申请发明专利 1 项。

当年新增的重要科研任务：

序号	课题名称	项目（课题）编号	负责人及单位	起止时间	总经费（万元）	本年度实到经费（万元）	经费来源	类别	类型	研究方向
1	量子基础算法及其在密码分析中的应用	17-163-14-XZ-002-004-01	李洪波	2017.1-12	410	410	其他	主要负责	科技委项目	1
2	数学定理的机器证明和数学证明的验证补充	QYZDJ-SSW-SYS022	李洪波	2017.5-2022.5	100	10	中国科学院	主要负责	前沿科学重点研究项目	1
3	几何定理机器证明的代数方法的等价性与完全性	11671388	李洪波	2017.1-2020.12	48	24	基金委	主要负责	面上项目	1
4	CXJJ-17-M142	CXJJ-17-M142	冯秀涛	2017.1-2019.1	60	30	中国科学院	主要负责		2
5	区块链抗量子加密技术研究		冯秀涛	2017.8-2019.7	60	24	北京太一云科技有限公司	主要负责	其他	2

经费来源：科技部、基金委、中科院、其他
类型：指计划名称，如：973 计划，863 计划，国家科技重大专项、科技支撑计划、国家自然科学基金、国际合作项目、公益性行业科研专项等
类别：主要负责、参与
研究方向：与第一部分实验室基本情况列表中的研究方向对应，填写研究方向序号。

2.代表性研究工作进展

代表性工作 1	名称	本实验室固定人员参加名单	所属研究方向
	差分 Galois 群的特定化	冯如勇	差分 Galois 理论
简要介绍	Galois 群的特定化问题研究：什么时候方程的 Galois 群的特定化等于方程特定化的 Galois 群？换言之，什么时候计算 Galois 群与特定化这两种“运算”是可交换的？这个问题,可追溯到 Hilbert 关于经典 Galois 理论的反问题的研究。这一问题的解答可以证明：要解决有理数域 Q 上的反问题，只需要解决有理函数域 Q(t)上的反问题。 在线性微分方程情形，当常数域为有理数域 Q 时，Grothendieck 在考虑线性微分方程的代数函数解时，提出了如下猜测：线性微分方程的解都是代数函数当且仅当对于几乎所有的素数 p，模 p 后所得方程的解都是有理函数。1982 年，Katz 提出了一个与上述猜测等价的猜测，被称为关于 p-curvature 的 Grothendieck-Katz 猜测，目前还没有被完全解决。而对于线性差分方程，没有相应的 Grothendieck-Katz 猜测。 2002 年在 Invent. Math.上，Lucia 证明了 q-差分方程情形的 Grothendieck-katz 猜测。Hrushovski 在 2002 年解决了常数域为函数域时微分 Galois 群的特定化问题。他证明：总存在特定化，使得微分 Galois 群的特定化等于微分方程特定化的 Galois 群，并进一步刻画了这些特定化。 我们对于函数域情形的线性差分方程，解决了 Galois 群的特定化问题。我们证明了:存在特定化，使得差分 Galois 群的特定化等于线性差分方程特定化的 Galois 群，并且刻画了这些特定化。 差分 Galois 理论问：什么样的群是线性差分方程的 Galois 群。对于该问题，权威专家 van der Put 与 Singer 于 1997 年提出了如下的猜想（van der Put-Singer 猜想）:假设 G 是 GL_n(C) 中的代数子群，这里 C 是特征为零的代数闭域,那么 G 是定义在 C(x) 上的线性差分方程的 Galois 群当且仅当商群 G/G^\circ 是循环群，这里 G^\circ 是 G 的含么连通分支。通常称 C(x) 为方程的基域。该猜想只在基域为 C(x) 时的某些特殊情形得到证明，一般情形还有待于解决。 利用上面关于差分 Galois 群特定化的结果，我们证明了:若 van der Put-Singer 猜想在 C 为复数域时成立,那么它在 C 为任意特征为零的代数闭域时也成立。这样，将问题归结为 C 为复数域情形。在该情形，我们有望利用解析的工具，最终证明 van der Put-Singer 猜想。		

代表性工作 2	名称	本实验室固定人员参加名单	所属研究方向
	D-有限函数的理论与算法	陈绍示	符号计算与组合数学

简要介绍	D-有限函数是以多项式为系数的线性微分方程的解,又称 Holonomic 函数。这类函数是美国科学院院士、MIT 组合学家 Stanley 在 1980 年引入的,在其关于计数组合学的经典著作中系统地介绍了这类函数的基本性质及组合应用。 许多组合数学与数学物理中常用的特殊函数都是 D-有限的,如代数函数、超几何函数等。D-有限函数具有丰富的代数与解析性质。在代数方面,Stanley 在 1980 年证明了这类函数全体构成一个代数;在解析方面,D-有限函数的奇点只依赖于方程本身而与初始值选取无关,并且系数的渐近性态可以由奇点很好的刻画。多变元 D-有限函数的基本理论是 20 世纪 90 年代在 Gessel, Zeilberger, Lipshitz 等人的工作中发展的,并与 Bernstein 与 Kashiwara 等人发展的代数 D-模理论有密切联系。 2017 年,我们在 D-有限幂级数的理论与算法两方面取得了如下成果: 1、多变元 D-有限幂级数的有理性定理 幂级数的算术理论是 Fatou, Poyla, Szego 等人在 20 世纪初发展起来的,其核心问题是研究幂级数的超越性与有理性。在组合分析中,作为生成函数的幂级数的算术性质可以揭示组合序列的内在结构,但是判定这些性质往往是很困难的。 有理-超越二分定理将超越性判定转化成非有理性判定,大大降低了判定问题的难度。在幂级数的有理性研究方面,两个著名的定理是 Szego 定理与 Polya-Carlson 定理。这些经典的结果往往局限于单变元情形。 从 2016 年开始,我们与滑铁卢大学 Jason P. Bell 教授开展了关于多变元 D-有限幂级数的有理性方面的研究。2017 年,我们证明了系数取自有限集合的多变元 D-有限幂级数必然是有理函数的幂级数展开。该结果是多变元 Szego 型定理,将 1996 年 van der Poorten 与 Shparlinski 的有理性定理从单变元推广到了多变元。论文发表于组合理论方面最权威的杂志 Journal of Combinatorial Theory, Series A. 代表性论文:Jason P. Bell and Shaoshi Chen. Power Series with Coefficients from a Finite Set. Journal of Combinatorial Theory, Series A, 151: 241–253, 2017. 2、Fuchsian D-有限函数的约化算法与邻差算子计算 Wilf-Zeilberger 理论现已成为符号计算应用于组合数学、特殊函数论、数学物理等领域的桥梁。该方法的核心步骤是对给定的多变元函数构造出单变元的多项式系数的线性微分或差分算子。该算子被称为给定函数的邻差算子。 目前与该理论相关的研究问题主要有两方面:一方面是对于给定特殊函数,如何判定邻差算子是否存在,即存在性问题;另一方面是在邻差算子存在的前

	提下，如何有效地计算出邻差算子来，即构造性问题。在邻差算子的构造方面，已有算法的共同特点是：在计算邻差算子的同时不可避免地需要计算相伴的验证函数，而该函数一般在存储大小上比邻差算子高出一个量级，并且在应用中往往是多余的。一直以来，如何将邻差算子的计算与验证函数的计算分离开来，是一个很具挑战性且重要的问题。解决这个分离问题的关键是约化算法。 从 2010 年开始，我们在一系列工作中发展并完善了基于约化的计算邻差算子的第四代算法。我们在 2016 年的工作中给出了基于约化的计算代数函数邻差算子的高效算法。 如果 D-有限函数只有正则奇点，则称为 Fuchsian 的。代数函数是特殊的 Fuchsian D-有限函数。在 2017 年，我们提出了 Fuchsian D-有限函数的加法分解的概念，并提出了相应的约化算法。基于该约化算法，设计了计算双变元 Fuchsian D-有限函数邻差算子的高效算法。文章已被符号计算权威杂志 Journal of Symbolic Computation 接收。 该项工作最近又由法国数学家 van der Hoeven (ICM2018 45 分钟邀请报告人) 推广到一般 D-有限情形，并在其文中提到：“The existence of normal confined reductions has also been shown in increasingly general cases and most noticeably so for Fuchsian differential equations [4, 3]” (这里所引文章 [4,3] 都是本人与合作者的工作)。 代表性论文：Shaoshi Chen, Mark van Hoeij,Manuel Kauers, Christoph Koutschan. Reduction-based Creative Telescoping for Fuchsian D-finite Functions. Journal of Symbolic Computation, 85: 108－127, 2018.

代表性工作 3	名称	本实验室固定人员参加名单	所属研究方向
	对称密码设计与分析	冯秀涛	对称密码
简要介绍	针对 Perrin 等人在 2016 年美密会上提出的 Butterfly 结构 4 差分 S 盒具有最优非线性的猜想，我们推广了 Butterfly 结构，并证明了推广的 Butterfly 结构同样具有 4 差分均匀度和最优的非线性度，从而彻底证明了 Perrin 等人在 2016 年美密会上提出的猜想。相关结果发表在对称密码领域国际顶级会议 FSE 2018。 针对 CAESAR 认证密码第三轮候选算法 ACORN，我们在故障模型下给出了针对 V2 和 V3 两个版本的安全性评估结果。结果表明：在随机故障模型下，相对于 V2 版本，V3 版本具有更弱的抗故障差分分析能力。相关结果分别发表在 SCI 刊源 Security and Communication Network 和 The Computer Journal。 针对采用模加运算的对称密码算法在差分故障分析时导出的一类差分故障模型，我们在故障差分随机均匀分布假设下研究了其解个人的统计规律和解个数与注入故障之间的相互关系，给出了其解个数的数学期望和方差。我们的研		

	究结果进一步表明，在差分随机分布假设下，攻击者只需注入 ln(n)+5 个随机故障便可以确定方程系统的候选解。论文发表在中国科学 A 辑数学期刊。 针对一类以本原多项式的平方为特征多项式的线性反馈移位寄存器，我们给出了其圈结构、共轭对分布和连接图，并基于其构造了一大批具有极大周期的新的 de Bruijn 序列。相关结果发表在 SCI 刊源 Chinese Journal of Electronics。

代表性工作 4	名称	本实验室固定人员参加名单	所属研究方向
	计算代数几何及其在 CAGD 中的应用	贾晓红	计算代数几何
简要介绍	1.曲线曲面的μ基理论新进展。 参数形式与隐式形式是 CAGD 中曲线和曲面的主要表示方式。因这两种表示各自的优势与不足，在几何计算及造型中，人们常须要在二者之间相互转换，即参数曲线曲面的隐式化及隐式曲线曲面的参数化。这两种转化方式是 CAGD 中最基础且重要的问题。由此产生的一个更重要且具有挑战性的问题是：如何寻求新的曲线曲面的表达形式，使其兼具参数方程和隐式方程的优点，且完全传承原曲线曲面的信息，从而从根本上避免了不同形式之间复杂的转换过程。计算几何领域的著名学者 Thomas Sederberg 在 1995 年计算机图形学顶级会议 Siggraph 上指出：寻找新的曲线曲面表达形式将对持续了超过一世纪的隐式化问题带来根本性变革。 九十年代末，著名代数几何学家 David Cox，Thomas Sederberg 及陈发来将代数学中的合冲模理论与 CAGD 中的动曲线动曲面理论结合，提出了曲线曲面的μ基理论。在代数上，μ基是有理曲面的合冲模的一组基；在几何上，μ基是交成该曲线或曲面的一对动直线或一组动平面。因此，μ基理论又称合冲模理论或动曲线动曲面理论。μ基是联结曲线和曲面的参数表示与隐式表示之间的桥梁，是除参数形式、隐式形式之外的一种全新的有理曲线曲面的表达形式。它承载了曲线和曲面的所有内蕴几何性质，因其次数低、计算快、提供信息无冗余的特点，为很多曲线和曲面相关的几何计算问题提供了全新的快捷途径。μ基理论建立了代数几何与几何建模领域的联系。在其发展的十多年历程中，平面有理曲线、空间有理曲线、有理曲面的μ基的存在性证明顺次破冰，随之而来的最重要的研究问题集中在如何运用 μ 基简化几何建模中的某些重要问题，包括曲线曲面的快速紧致隐式化、奇异点计算、点逆公式表达等。近年来，μ基理论也逐渐被用于曲线曲面对应理想的 Rees 代数结构的分析中。 我们在上述μ基相关的重要问题上作出了一系列工作。2017 年我们完成了 canal 曲面的 μ 基理论研究。canal 曲面广泛应用于工业环境中，是计算机辅助几何设计与计算机图形学中的重要研究对象。我们给出三个运动平面的显式表达，它们的系数向量的外积是该曲面的参数方程，它们的结式是该曲面的隐式方程，它们可直接给出曲面上点所对应的参数的表达式，也可给出曲面上奇		

	异点轨迹的表达式。部分成果写入申请人与其合作者的英文专著《Essentials in Commutative Algebra》中，部分成果发表在计算数学重要期刊《Journal of Computational and Applied Mathematics》上：X. Jia, X. Shi and F. Chen. Survey on the Theory and Applications of μ-Bases for Rational Curves and Surfaces. Journal of Computational and Applied Mathematics, Vol. 329, 2-23, 2018. 2.两椭球构型的穷举、判定、分层及连通图。 碰撞检测问题的核心是两几何体位置关系的判断。因现实世界中物体的几何形状复杂，通常的做法是用简单包围体做近似。包围体的选择有立方体、球体、椭球等，因此研究两椭球的相对位置关系对于一般碰撞检测问题十分重要。 相对位置关系有三个不同层次：(1) 分离、相交或包含，这也是最简单基本的关系；(2) 交线的形态分析，这可对相交情形下的椭球进一步细化其相交的具体情形；(3) 交体的构型分析，这将彻底反应两椭球地位的不对等性，突破传统碰撞检测仅研究相对位置关系而不区分两几何体的不对等性的局限。 我们彻底解决了以上全部问题。我们通过符号计算的手段给出结论的显式表达，从而在最后一步结果之前不存在误差累计的问题，在整个过程可将检测误差降到最低。我们首次给出了交体构型的穷举（20 种），及根据交体奇异程度的分层，并给出了 20 种构型的联通图—即构型在两椭球连续变化的情况下的可能走向。这一系列结论对于机器人学、分子排列等应用很重要。

代表性工作 5	名称	本实验室固定人员参加名单	所属研究方向
	数控加工中的轨迹规划	袁春明	高档数控中的数学机械化方法
简要介绍	在数字化设计与制造中，CAM（计算机辅助制造）是非常重要的一部分。对于建模之后的自由曲面，需要通过 CAM 规划刀具路径以及刀轴方向，然后通过 CAD 进行速度规划，最后生成数控机床可以识别的加工指令。对于给定的自由曲面，如何规划刀具路径以及每个刀触点处的刀轴方向，一直是国内外学者们的研究焦点。 当数控加工涉及复杂造型时，需要五轴数控机床来进行加工。五轴数控加工的路径规划是数控加工的基本问题之一。对于五轴数控加工而言，路径规划非常复杂，既需要规划刀心点的轨迹，又需要规划刀轴的方向。对于球头刀来说，两者在一定程度上可以分开进行规划。但是对于其它刀具，如平底刀或者环形刀，两者是紧密耦合在一起的。在未知刀轴方向的前提下，直接进行刀心点的轨迹规划，是一项非常困难的工作。对于设计的刀具路径，希望最终的路径较短且较为光滑，以达到较高的加工的效率和加工质量。 我们首先考虑每个刀位点的刀姿可行域(C-space)，以此计算出整个加工		

	曲面上的可行的光滑刀姿，达到光滑化刀姿的目的，然后根据每个刀位点的刀姿，设计光滑的刀具路径，同时考虑加工的效率和残高约束。这样，我们既可以兼顾加工的效率(带宽)和路径的光滑性，使得得到的刀具路径既有总路程较短且路径光滑的特点，又兼顾了相邻路径的相似性。 对于数控中给出的 G01 代码，其插补问题是数控加工中的一个基本问题。如果针对 G01 代码表示的折线段直接加工，那么加工的质量会比较差，加工速度较为缓慢。之前我们设计了针对平面 G 代码的二次 B 样条拟合方法。但目前大多数的 G 代码是空间形式的，如何设计相应的拟合算法是较为困难的问题。 我们给出了空间拟合曲线段与空间折线段之间的 Hausdorff 距离的精确计算方法，给出了误差可控的三次 B 样条拟合算法。进一步，我们通过引入时间参数和动力学约束，给出了严格满足距离误差精度以及速度、各轴加速度和加加速度约束下的时间样条拟合曲线，它具有最短加工时间。

列出本年度 3-5 项代表性研究工作，表格可复制。

3.合作研究的组织情况与实施效果

（简要介绍实验室一年来开展合作研究的情况和标志性成果,组织和参与国际重大科学研究计划的情况（指正式签订协议书的国际合作科研项目）及成效。）

主要合作研究项目为科技委项目“量子基础算法及其在密码分析中的应用”，合作单位包括中科院软件所、中科院计算所、南开大学、山东大学。标志性成果是有限域上非线性方程组求布尔解的量子算法及其在经典密码体系分析中的应用。

二、队伍建设和人才培养

1.队伍结构与团队建设

（简要介绍实验室队伍的总体情况，包括学术带头人（课题组长）人数，队伍结构，特别是 40 岁以下研究骨干比例及作用。评估期内队伍建设、人才培养（包括青年人才、研究生培养）与引进情况，特别是团队组织和凝聚、吸引、培养国内外优秀中青年人才的措施及取得的成绩。各主要方向 40 岁以下研究骨干承担科研任务情况及取得的研究成果情况等。）

实验室现有固定科研人员 26 人，其中研究员 12 人、副研究员 8 人、助理研究员 3 人，包括中国科学院院士 3 人（吴文俊、万哲先、李邦河）、杰出青年基金获得者 2 人（高小山、李洪波）、“百人计划”入选者 2 人（高小山、李洪波）、“青年千人”入选者 1 人（叶科）。

2017 年实验室引进叶科副研究员。他入选第十四批国家“千人计划”青年项目、中国科学院百人计划 C 类、中国科学院优秀青年人才。引进之前，叶科为美国芝加哥大学数学系 L.E.Dickson 讲师和统计系的博士后，合作导师是著名应用代数几何专家 Lek-Heng Lim 教授。近几年，叶科在结构矩阵计算、张量代数及其交叉应用领域做出了杰出的工作。

实验室 2017 年在读硕士 23 人，在读博士 33 人，毕业博士 11 人，毕业硕士 3 人，其中温子超获得中科院院长特别奖,陈勇获得国家奖学金,付士辉获得数学院院长奖学金优秀奖,

张国强、荆瑞娟获得获得阿美奖学金特等奖。

实验室 40 岁以下研究骨干承担科研任务情况及取得的研究成果情况介绍：

冯如勇：基金委面上项目和中科院青年创新促进会项目的负责人。本年度研究工作：见此前的代表性工作 1。

张志芳：研究工作主要在两个方面开展，一是局部修复码，另一个是保密信息提取。本年度主要研究成果：1. 将经典编码理论中的堆球界用到局部修复码定义的局部修复空间中，结合 MacWilliams 等式，得到二元 LRC 码的堆球界。该界优于 C-M 界，而且是显式可计算的。进一步，去掉了互不相交的局部修复集合的假设，分别得到 r=2 和 d≥5 时的显式参数界。2.设计了一般的达到 PIR 容量的线性 PIR 方案，所需分包数为 dnM-1，而 Sun & Jafar 的方案需分包数 NM，我们减少了因子 1/ndM-1，其中 d=gcd(N,T)，n=N/d。证明了任意达到容量的线性 PIR 方案分包数 ≥ dnM-1，从而我们给出的方案达到最优分包数。从 PIR 方案所基于的有限域大小来看，我们的方案比 Sun & Jafar 用到的有限域小了因子 1/NdM-2 。

袁春明：中科院青年创新促进会项目和广西玉柴数控项目的负责人，同时也是实验室量子计算与密码分析项目的核心成员。本年度的工作见此前的代表性工作 5。

贾晓红：虚拟现实环境中的碰撞检测理论研究项目的负责人。本年度的研究工作见此前的代表性工作 4。

冯秀涛：基金委面上项目、中科院保密项目、61569 部队委托项目以及北京太一云科技有限公司委托项目的负责人，同时也是实验室量子计算与密码分析项目的核心成员。本年度主要研究成果见此前的代表性工作 3。

陈绍示：基金委青年项目的负责人，同时也是实验室量子计算与密码分析项目的核心成员。本年度在科研方面，主要在幂级数的有理性定理，组合恒等式的机器证明，以及微分方程的奇点分析三方面取得进展。具体研究结果见此前的代表性工作 2。

叶科：实验室量子计算与密码分析项目的核心成员。本年度研究工作：1.研究了张量网状态的复杂度。我们定义了张量网秩，并通过代数几何的工具研究了张量网秩的一些性质。同时我们还计算了一些常见的张量的张量网秩，例如矩阵乘法张量，W-状态以及 GHZ 状态。2.研究了仿射 Grassmann 流形上的优化算法。我们将仿射 Grassmann 流形作为一个 Zariki 开集嵌入到高维的 Grassmann 流形中，并以此诱导了黎曼度量。利用这个黎曼度量，我们在仿射 Grassmann 流形上给出了测地线，距离函数，梯度函数等一系列几何量的计算公式，并给出了在仿射 Grassmann 流形上的优化算法。3.研究了张量特征值的反问题，即对于任意给定的有限多个复数，是否存在一个张量 T，使得 T 的特征值就是给定的这些复数。我们利用代数几何的工具证明了这个问题在大多数情况下是无解的，同时列举了所有有解的情况。

潘彦斌：基金委面上项目的负责人，同时也是实验室量子计算与密码分析项目的核心成员。本年度在科研方面的工作如下：1、和学生李昊宇合作的论文被 WISA 接收，给出了搜索版本 SMP 问题到其优化版本的确定性归约，并且该归约只调用一次优化版本 SMPoracle。2、分析了 2008 年 PKC 上提出的一个签名体制的安全性，指出了作者认为更安全的随机版本实

际上在安全性方面有一定的问题，在选择消息攻击模型下，利用格基约化算法，我们可以成功恢复出私钥。3、提出了一个新的计算 Hermite 标准型的启发式算法，在现实运行中表现得很好，在高维情况下比 NTL 中实现的算法要快得多。基于一个更弱的假设下，新算法的时间复杂度基本上和计算矩阵乘法的时间复杂度差不多。对随机理想格计算 Hermite 标准型时，其简单标准型所占的比例通常要高于一般的随机矩阵，因此，我们开始从理论上分析，最终得到了随机理想格中简单 Hermite 标准型密度的表达式，发现与代数数域中的类数公式相关。

李博：基金委青年项目的负责人，同时也是实验室量子计算与密码分析项目的核心成员。本年度研究工作如下：1.概率布尔网络（Probabilistic Boolean Network）是刻画基因调控的基本模型。1969 年，Kauffman 提出了著名的随机布尔网络，基因之间开和关的状态演化由初始随机化的布尔函数决定。这一模型开启了对基因调控网络（Gene Regulator Networks）的系统研究。概率布尔网络在每一时刻重新随机化布尔函数，是 Kauffman 模型的重要推广，并在近年的计算机网络，社会网络，人工智能等基础领域有广泛的应用。但是，一个难点是，概率布尔网络的绝大多数定量刻画问题都是 NP 困难问题。所以，目前很少有结果能够突破这一计算能力上的界限，对概率布尔网络的行为给出清晰的，具体的刻画。我们注意到，在 Kauffman 模型中，很多情况下一个基因每次仅与几个（2 个或 3 个）基因发生作用。基于基因调控网络的这个特点，我们提出了一个简化的基于 gossip 过程的概率布尔网络，每时每刻仅有一对基因（点）发生相互作用。该模型继承了概率布尔网络的核心结构，并且将经典 gossip 过程包含为一特例。基于此模型，我们用图论理论和组合分析理论建立了一系列定理。文章被国际顶级的网络科学杂志 IEEE/ACM Transactions on Networking 接收。2．量子网络是一个在量子计算和量子通信中新兴的研究方向。能否像控制经典网络一样实现量子网络的状态精确操作和存储是未来量子技术能否展现其全部理论潜力的关键。特别的，量子局域测量经典通信（Local operation classical communication quantum network）是很多量子计算和量子通信模型的基础。基于量子网络的计算和通信是国际学术界量子网络领域一个新兴的研究热点。计算机网络和网络控制中的一致算法，现在已经有了深刻的理论认识，而量子 consensus 算法和量子 gossip 算法则处于基础理论建立时期。我们研究了一类特殊的量子混杂网络，该类网络中，每个结点上有一个量子比特。我们找到一种方法利用局部投影测量并通过经典的通讯网络交换测量结果，最终使得网络中每个结点上的量子比特状态达到一致。我们提出了一种分布式的算法，证明了网络中的每个结点所持有的量子比特在几乎处处的意义下最后的状态达到一致。相关论文发表在 Scientific Reports。

李伟：本年度研究工作如下：1.Kolchin 多项式的可定义性(Definablity in families)：在微分闭域的模型理论研究中，各种微分指标(秩)的是否可定义性问题是微分代数学家与模型论专家共同关注的研究热点。例如，Pillay 与 Nagloo 证明了 Morley 秩、Lascar 秩与微分 Krull 维数都是不可定义的。Kolchin 多项式，也称微分维数多项式，是微分代数簇或微分可构造集的一个非常重要的双有理不变量。我们证明了 Kolchin 多项式的可定义性，即对于任意给定的一族含参微分簇，具有固定 Kolchin 多项式的微分簇集合是一个微分可构造集。作为推论，证明了微分簇的弱不可约性是可定义的。 2.应用模型论证明了微分周簇的存在性，从而完全解决了微分代数几何中的相关公开问题，将代数周簇理论推广到了微分情形，填充了微分模空间(moduli space)研究的空白。相关论文“Differential Chow Varieties Exist”发表在 J. Lond. Math. Soc.3.偏微分周形式理论：发展了偏微分代数几何中的相交理论，证明了偏微分相交定理；定义了偏微分周形式，证明了它的基本性质，并证明了一类偏微分周簇的存在性。

2.实验室主任和学术带头人简介

（依次简要介绍实验室主任、副主任、学术带头人和优秀青年骨干的情况，在实验室发挥的作用以及在国家科技计划担任咨询专家情况。）

姓名	李洪波	身份类型	实验室主任
性别	男	年龄	49
最后学位	博士	获得最后学位所在院校	北京大学
任职时间	2009	依托单位职务	
学习及工作经历	1984.9-1988.7 北京大学本科 1988.9-1991.7 北京大学硕士 1991.9-1994.7 北京大学博士 1994.8-1996.7 中国科学院系统科学研究所 博士后 1996.8-1998.7 Arizona State University 博士后 1998.8-1998.12 中国科学院系统科学研究所 研究员 1998.10-1999.12 Christian-Albrecht Universitaet zu Kiel 访问教授 1999.1-至今中国科学院数学与系统科学研究院 研究员 2001.7-2001.12 Christian-Albrecht Universitaet zu Kiel 洪堡学者		
研究方向	几何推理		
代表性工作	主要研究数学机械化及其应用，侧重几何代数、经典不变量理论与算法，及其在机器证明、几何重建、数控中的应用。他建立的几何定理证明的 Clifford 代数方法和高级不变量理论，拥有功能强大的高层计算手段，克服了基本不变量无法克服的许多计算困难；应用它们证明和扩展经典几何和微分几何定理，使得以前数十万项都难以完成的计算，现在只要一两项就能完成，极大地提高了数学机械化方法的效率。他合作建立了共形几何代数，为各种经典几何提供了统一、简洁的几何语言，被欧美多个国家的学者用于数学、理论物理等基础研究领域，以及计算机图形学、计算机视觉、机器人等高技术领域。他合作提出基于数学机械化方法的数控插补与刀补的高效算法，在国家重大专项支持的蓝天数控系统中实现，获国家发明专利 6 项。		
个人荣誉	国家杰出青年科学基金，百千万人才工程国家级人选，中科院百人计划，国务院政府特殊津贴专家，香港求是杰出青年学者奖，David Hestenes 奖，ACM SIGSAM ISSAC 杰出论文奖，中科院数学院关肇直首席研究员		
学术兼职	全国工业机械电气系统标准化技术委员会安全控制系统分技术委员会委员，北京数学会理事		
学术期刊兼职	《Advances in Applied Clifford Algebras》编委，《Journal of Systems Science and Complexity》编委		

姓名	高小山	身份类型	学术带头人

性别	男	年龄	54
最后学位	博士	获得最后学位所在院校	中国科学院系统科学研究所
任职时间	2017	依托单位职务	常务副院长
学习及工作经历	1980.9-1984.6 国防科技大学 本科 1984.9-1988.6 中国科学院系统科学研究所博士 1988.9-1990.12 美国德克萨斯大学奥斯汀分校博士后 1988.7-1991.12 中国科学院系统科学研究所 助理研究员 1991.12-1996.12 中国科学院系统科学研究所 副研究员 1992.7-1996.12 美国威奇托州立大学 高级研究学者 1997.12-1998.12 中国科学院系统科学研究所 研究员 1998.12-至今 中国科学院数学与系统科学研究院研究员		
研究方向	数学机械化，自动推理，符号计算		
代表性工作	在几何自动作图方法，几何定理机器证明的消点法与微分系统的数学机械化方法等方面做出了突出成果。主要学术成果是： （1）几何自动作图方法：提出几何作图的系统、高效算法，突破了过去只用尺规作图的局限，使一大类问题得以快速求解；将数学机械方法由定理机器证明开拓到自动作图并得到重要应用。 （2）几何定理机器证明的消点法：合作建立消点法，首次实现可读证明自动生成，使几何定理机器证明进入到机器证明可以与传统证明媲美的新阶段。 （3）微分系统的数学机械化方法：建立了微分稀疏结式、周形式、差分特征列理论与高效算法，将数学机械化核心理论推广到微分/差分情形；实质性开拓了数学机械化方法的适用范围，是数学机械化研究的“突破”。		
个人荣誉	国家杰出青年科学基金，973 首席科学家，中科院百人计划，关肇直首席研究员，国家自然科学二等奖，中科院自然科学一等奖，求是杰出青年学者奖，中科院青年科学家一等奖，中科院盈科优秀青年学者奖，第 4 届亚洲数学技术大会最佳论文奖，国家十五重大科技成就网络展，中创软件人才奖，‘十一五’国家科技计划执行突出贡献奖，ACM SIGSAM ISSAC 杰出论文奖。		
学术兼职	中国数学会副理事长，中国工业与应用数学会副理事长，国际工业与应用数学联盟成员委员会委员，系统工程学会副理事长，中国图学学会常务理事，中国密码学会密码数学专业委员会副主任，ACM SIGSAM Advisory Committee Board 委员，ICIAM Member Committee 委员，担任中央军委科技委国防科技创新特区领域专家。		
学术期刊兼职	《Journal of Systems Science and Complexity》主编，《Journal of Symbolic Computation》编委，《International Journal of Computers Communications & Control》编委，《Electronic Journal of Mathematics and Technology》编委，《中国科学：数学》编委，《计算机辅助设计与图形学学报》编委，《中国图象图形学报》编委，《中国高校应用数学学报》编委，《数学研究与评论》编委		

姓名	李子明	身份类型	实验室副主任
性别	男	年龄	55
最后学位	博士	获得最后学位所在院校	University of Linz, Austria
任职时间	2009	依托单位职务	
学习及工作经历	1980.9-1985.7 清华大学本科 1985.9-1988.7 中国科学院系统科学研究所硕士 1992.2-1996.4University of Linz 博士 1988.9-1992.1 清华大学讲师 1996.6-1997.8 中国科学院系统科学研究所副研究员 1997.9-1999.12Institut SCAI, GMD, St. Augustin 博士后 2001.11-2004.2 University of Waterloo 博士后 1999.12-2005.3 中国科学院数学与系统科学研究院 副研究员 2005.4-至今 中国科学院数学与系统科学研究院研究员		
研究方向	符号计算		
代表性工作	1、关于奥尔(Ore)多项式的高效算法 奥尔多项式是计算机处理线性常微分和差分算子的基本代数模型。我们把交换情形下的子结式理论推广到非交换奥尔多项式。从而给出了计算 Ore 多项式最大右公因子的模方法，克服了该计算过程中的中间表达式膨胀。利用子结式理论，给出了计算奥尔多项式最小左公倍式的高效算法。该算法不仅复杂度低，而且实际运算效率是目前最好的。相关工作被国际著名商用计算机代数软件 Maple 采用。 2、有限维微分-差分模的分解 有限维微分-差分模是计算机处理有限维线性偏微分和差分系统的基本代数模型。我们把常微分和差分伽罗华理论中的 Picard-Vessiot 扩张推广到多变元情形，给出了确定有限维微分-差分模所有非平凡子模的算法，其中确定一阶子模的算法获得 ACM SIGSAM ISSAC 杰出论文奖。 3、超指数-超几何项的加法分解 利用符号计算处理函数的一个基本问题是对它们在一定范围内积分和求和。加法分解不仅能在给定范围内计算积分与和式，还可以把在该范围内不可积和不可和的部分限制到最小。我们给出了计算超指数函数积分，超几何和 q-超几何项求和的加法分解。完成了从有理函数加法分解到无理函数分解的第一步。相关工作获得 ISSAC 2014 杰出 Poster 奖。 4、和差算子(telescoper)的存在与构造 和差算子是计算定积分和定和式的基本代数工具。我们给出了混合超几何项的乘法分解，并利用该分解给出了和差算子的必要充分条件。利用加法分解设计了最新一代（第四代）计算和差算子的方法。该方法可以避免计算规模较大的验证函数，显著地提高了计算和差算子的效率。		
个人荣誉	ACM SIGSAM ISSAC 杰出论文奖，ISSAC 2014 杰出 Poster 奖，中科院人事局朱李月华优秀教师奖		

学术兼职	中国数学会理事
学术期刊兼职	《Journal of Symbolic Computation》编委,《系统科学与数学》副主编

姓名	邓映蒲	身份类型	实验室副主任
性别	男	年龄	46
最后学位	博士	获得最后学位所在院校	北京大学
任职时间	2009	依托单位职务	
学习及工作经历	1989.9-1993.7 武汉大学 本科 1997.9-2002.6 北京大学 博士 1993.7-1997.7 桂林电子工业学院助教 2002.7-2004.5 中国科学院数学与系统科学研究院博士后 2004.6-2007.3 中国科学院数学与系统科学研究院助理研究员 2007.4-2013.2 中国科学院数学与系统科学研究院副研究员 2013.3-至今 中国科学院数学与系统科学研究院研究员		
研究方向	信息安全		
代表性工作	在密码与计算数论的交叉领域,研究有密码背景的计算数论以及基于数论的密码, 主要学术成果是： (1) 计算数论--素数判定与整数分解：给出了以前 9、10、11 个素数为基的最小强伪素数的精确值, 证明了张振祥教授的猜想；给出了三类特殊数的素性判定的二次确定性多项式时间算法；提出了整数分解问题的新算法。 (2) 代数数论：证明了在任意代数数域中 Exact 覆盖系的模数必然重复的 Kim 猜想；建立了任意代数数域的 order 上的类域论并给出应用。		
个人荣誉			
学术兼职	中国密码学会理事会常务理事,中国数学会计算机数学专业委员会委员, 中国电子学会信息论分会委员, 中国密码学会密码数学理论专业委员会		
学术期刊兼职	《密码学报》编委,《Journal of Systems Science and Complexity》编委,《系统科学与数学》编委		

姓名	支丽红	身份类型	实验室副主任
性别	女	年龄	48
最后学位	博士	获得最后学位所在院校	中国科学院系统科学研究所
任职时间	2014	依托单位职务	

学习及工作经历	1987.9-1991.6 北京大学 本科 1991.9-1996.6 中国科学院系统科学研究所 博士 2001.8-2002.7 加拿大西安大略大学博士后 1998.4-2001.3 日本爱媛大学 助理教授 1996.7-1998.12 中国科学院系统科学研究所助理研究员 1998.12-2003.3 中国科学院数学与系统科学研究院助理研究员 2003.4-2009.2 中国科学院数学与系统科学研究院副研究员 2009.3-至今 中国科学院数学与系统科学研究院研究员
研究方向	混合计算
代表性工作	国际上最早从事符号和数值混合计算的学者之一，在基于结构矩阵的基本代数运算的混合算法、数值多项式方程组奇异解的计算、精化和验证、有理函数全局最优解的可信验证方面取得了一系列突出成果，获得第七届中国青年女科学家奖。 近年来取得的重要成果： （1）提出了新的计算奇异多项式系统在孤立重根处的局部对偶空间基底的算法。新算法与规则化的牛顿迭代相结合，构造出了基于近似重根局部结构的广义牛顿精化算法。在理论上首次证明了新算法的二次收敛性。 (2) 将半定规划、大规模 Gram 矩阵的恢复和有理系数多项式平方和结合，给出准确的无数值误差的有理函数全局最优值的可信验证。对于带限制条件的最优问题，首次证明了在 一般坐标系下，多项式在可行域上非负当前仅当在构造的每一个截断代数簇上，可以写成多项式平方和。 （3）给出了基于实代数几何的第一个单指数复杂度新算法来判定和计算任意凸集中的有理点。并将新算法应用于判定一个非负整系数多项式是否存在有理系数多项式的平方和表示。给出美国伯克利大学 Bernard Sturmfels 教授问题反例的第一个计算机验证。
个人荣誉	第七届中国青年女科学家奖
学术兼职	中国数学会计算机数学专业委员会主任，中国数学会理事，ACM SIGSAM 副主席
学术期刊兼职	《Journal of Symbolic Computation》编委，《Mathematics in Computer Science》编委，《ACM Communications in Computer Algebra》编委，《SIAM Journal on Applied Algebra and Geometry》编委，《系统科学与数学》编委

姓名	冯如勇	身份类型	优秀青年骨干
性别	男	年龄	39
最后学位	博士	获得最后学位所在院校	中科院数学与系统科学研究院
任职时间		依托单位职务	
学习及工作经历	1996.9-2000.7 中国科学技术大学 学士 2000.9-2005.7 中国科学院数学与系统科学研究院博士 2005.7-2010.3 中国科学院数学与系统科学研究院 助理研究员 2010.4-至今 中国科学院数学与系统科学研究院 副研究员		

研究方向	微分差分 Galois 理论、符号计算
代表性工作	1、差分 Galois 理论中的正问题：正问题，即差分 Galois 群的计算问题，是差分 Galois 理论中的两个基本问题之一。我们首次给出了计算一般情形差分 Galois 群的算法（即给出 Galois 群的定义方程），从而解决了差分 Galois 理论中的正问题这一公开问题。结果发表于计算数学领域的优秀期刊 Mathematics of Computation。 2、Zeilberger 算法的终止性判定：Zeilberger 算法是 Wilf-Zeilberger 理论中的核心算法。该算法的终止性依赖于给定函数的邻差算子的存在性。我们对于双变元混合超几何项，给出了它们存在邻差算子的充要条件，从而解决了该情形 Zeilberger 算法的终止性问题。成果发表于符号计算领域最重要的杂志 Journal of Symbolic Computation。 3、线性微分差分混合方程的符号求解：微分差分方程的符号求解（通常指 liouvillian 函数解）是符号计算领域的热点问题。目前已有工作局限于线性微分或者线性差分情形，而对于混合情形缺乏系统研究。我们给出了线性微分差分混合方程存在 liouvillian 函数解的充要条件，并对于素数阶不可约方程给出了求解算法。成果发表于符号计算领域最重要的杂志 Journal of Symbolic Computation。
个人荣誉	2014 年中科院数学与系统科学研究院“突出科研成果奖” 2017 年吴文俊计算机数学青年学者奖，
学术兼职	中国数学会计算机数学专业委员会委员 第 10 届全国计算机数学年会，程序委员会共同主席 第 41 届国际符号与代数计算年会（ISSAC2016），程序委员会成员 第 6 届微分代数以及相关问题国际研讨会(DART6)，程序委员会共同主席。 第 39 届国际符号与代数计算年会（ISSAC2014）， Poster 委员会成员 第 10 届亚洲计算机数学会议（ASCM2012），程序委员会共同主席
学术期刊兼职	

姓名	袁春明	身份类型	优秀青年骨干
性别	男	年龄	37
最后学位	博士	获得最后学位所在院校	中国科学院数学与系统科学研究院
任职时间		依托单位职务	
学习及工作经历	1998.9－2002.7 中国科学技术大学学士 2002.9－2007.7 中国科学院数学与系统科学研究院博士 2007.7-2013.2 中国科学院数学与系统科学研究院助理研究员 2013.3-至今中国科学院数学与系统科学研究院 副研究员		
研究方向	符号计算,数学机械化,构造性微分-差分代数,计算机辅助设计与制造		

代表性工作	主要从事微分-差分方程的消去理论与算法研究。研究兴趣包括微分、差分方程的符号计算方法和复杂度分析，数控技术中的机械化方法等。 合作发展了微分差分方程的特征列方法与预解式理论，建立了微分差分吴-Ritt 整序原理和微分差分吴-Ritt 零点定理，解决了微分差分根理想成员问题，提出了基于微分差分方程的恒等式机器证明方法。另外还发展了差分方程组的预解式理论，将数学机械化的主要工具—特征列方法—推广到一类新的方程类型，是数学机械化研究的重要进展，被差分代数创始人 R.M. Cohn 认为是“解决了一个基本(fundamental)问题”。 合作建立了微分 Chow 形式理论，给出了一般(generic)微分多项式的相交理论，给出了扩展(generalized)微分 Chow 形式的定义及基本性质，以此为基础，首次给出了非线性微分结式的严格定义，并证明了一系列基本性质。相关论文在 Trans of AMS 上发表，审稿人认为：“这是一篇重要的、开创性(ground-breaking)的文章,有可能极大地推动微分代数几何的深入研究。作为代数周形式的一个引人入胜(intriguing)而又完全自然的推广，微分周形式应该引起代数几何学家们的重视。建立微分周形式的性质需要独创力(ingenuity)和对微分消去理论的全面知识。” 合作首次给出了微分 sparse 结式的概念，给出了一个关于给定微分多项式的个数、阶数与结式次数的单指数算法，获得了 ISSAC 2011 唯一杰出论文奖。授奖词完整地总结了这项工作：“微分多项式系统结式是微分代数和结式理论中一个重要、困难与全新（original）的问题。作者首次严格定义了微分结式与稀疏微分结式，证明了稀疏微分结式的一些重要性质，并设计了一个计算稀疏微分结式的单指数时间算法。该高效算法将会对应用数学与计算机科学中的若干问题起到影响，我们预计这篇文章将会阐明并开启（shed light on）微分代数、结式理论、复杂性理论、线性代数和组合学中新问题的研究。” 接着这一工作，合作深入研究了 Laurent 微分多项式系统的稀疏结式，给出了计算稀疏微分结式的关于输入规模的单指数复杂度算法。这一工作发表在 Foundations of Computational Mathematics 上。进一步地，合作将稀疏结式理论推广到差分情形。 在计算机辅助设计与制造方面，高速高精数控需要考虑在机床的基本性能与加工过程中的动力学性能的约束下，如何设计时间最优的速度函数，即速度规划。针对这些问题，应用微分方程理论与优化方法，合作在几种重要的情况下，提出了最优速度的高效计算方法。实验表明，这些算法比之前使用的算法效率提高了 60%-150%。相关结果发表在数控重要杂志 Robotics and Computer-Integrated Manufacturing 等。
个人荣誉	(1) 卢嘉锡青年人才奖，中国科学院，2014 (2) 获 ACM/SIGSAM 颁发的 ISSAC 2011 杰出论文奖，2011 (3) 入选首届陈景润未来之星计划，2009

学术兼职	<系统科学与数学> 编委

姓名	冯秀涛	身份类型	优秀青年骨干
性别	男	年龄	39
最后学位	博士	获得最后学位所在院校	中国科学院大学
任职时间		依托单位职务	
学习及工作经历	1996.09-2000.06 西安理工大学 学士 2000.09-2003.06 武汉大学 硕士 2003.09-2006.06 中国科学院大学 博士 2006.07-2008.03 北京握奇研究院 2008.03-2012.02 中科院软件所项目聘用人员 2009.12-2012.02 中科院软件所博士后 2012.02-2016.02 中国科学院数学与系统科学研究院助理研究员 2016.03-至今 中国科学院数学与系统科学研究院副研究员		
研究方向	对称密码		

代表性工作	近几年主要围绕序列密码设计与分析展开工作。在承担项目方面，作为项目/子课题负责人，承担了包括国家自然科学基金、科技部重大专项在内的 9 项项目的研发；共撰写了 2 套国际/国家标准草案，其中包括国际标准 1 套(含 4 项)，国家标准 1 套(含 3 项)；已申请发明专利 13 项，授权专利 7 项，其中国际发明专利 2 项，国防发明专利 2 项，国家发明专利 9 项。主要代表性工作有： 1.在序列密码算法设计方面，作为核心人员，参与了祖冲之算法(ZUC)的研制和国际标准化推进工作。序列密码祖冲之算法(ZUC)是 3GPP 的 4G 通信标准 LTE 的第三套机密性和完整性算法规范的核心算法，也是我国的 4G 移动通信加密标准。作为祖冲之算法的设计者之一，在祖冲之算法国际标准化推进期间，担任祖冲之算法国际标准化推进组成员和欧洲祖冲之算法安全评估专家组成员，负责祖冲之算法的修订工作并提出修正方案，组织祖冲之算法的技术分析和安全评估工作，并给出祖冲之算法的弱密钥分析、线性区分分析和代数分析等分析方法，为祖冲之算法国际标准化推进成功作为突出贡献。与此相关的成果主要包括：撰写祖冲之相关算法国际标准 4 项，起草国家行业标准草案 3 项，申请相关专利 4 项，并在对称密码国际顶级会议 FSE 2011 上发表论文 1 篇。 2.在序列密码算法破译方法方面，针对 ESTREAM 胜选算法 SOSEMANUK 和 Rabbit 提出面向字节的猜测确定分析方法，前者发表在三大密码学会之一的亚密会上，并彻底破译了包括 A2U2、Sablier、FASER128、FASER256、PANDA-s 等在内的一系列序列密码算法，其中对 FASER128/256 和 PANDA-s 的分析工作，导致它们在 CAESAR 竞赛中被淘汰。 3.在序列密码部件研究方面，给出了模 2n-1 加法的线性逼近的确切公式以及特征为 2 的有限域上的迹逆函数的代数免疫度的确切值，证明了 D.K. Dalai 关于其代数免疫度的相关猜想，推广了 Perrin 等人在 2016 年美密会上提出的 Butterfly 结构，并证明了这类结构同样具有 4 差分和最优非线性度等特性，从而彻底解决了 Perrin 等人在 2016 年美密会上提出的猜想。
个人荣誉	国家科技发明二等奖
学术兼职	CTCIS 2016 PC member，CTCIS 2017 PC member
学术期刊兼职	无

姓名	贾晓红	身份类型	优秀青年骨干
性别	女	年龄	36
最后学位	博士	获得最后学位所在院校	中国科学技术大学
任职时间		依托单位职务	

学习及工作经历	2000.9-2004.7 中国科学技术大学数学系 本科 2004.9-2009.7 中国科学技术大学数学系 硕博连读 2007.8-2009.7 美国莱斯大学计算机系博士联合培养 2009.9-2011.9 香港大学计算机系博士后 2011.10-2015.3 中国科学院数学与系统科学研究院助理研究员 2015.3-至今 中国科学院数学与系统科学研究院副研究员
研究方向	计算机辅助几何设计
代表性工作	计算代数几何方面的代表性工作为有理曲线曲面的μ基理论;计算机图形学方面的代表性工作为碰撞检测及曲面蓝噪声采样系列问题。截至目前，申请人已发表英文专著《Essentials in Commutative Algebra》《Commutative Algebra: An Introduction》两部，发表论文共二十余篇，其中 SCI 论文 17 篇，包括计算机辅助几何设计的最权威期刊《Computer Aided Geometric Design》，计算数学领域的重要期刊《Journal of Computational and Applied mathematics》，符号计算领域的最权威期刊《Journal of Symbolic Computation》，计算机图形学的权威期刊《Computer Graphics Forum》,《Computers & Graphics》,《Graphical Models》等。
个人荣誉	2009 年中国科学院院长奖优秀奖 2010 年中国科学院优秀博士论文 2011 年全国百篇优秀博士论文提名 2011 年中科院数学院海外优秀青年人才计划 2014 年国际会议 Shape Modeling International (SMI) 最佳论文提名 2014 年中科院数学院系统所关肇直青年研究奖 2017 年中国工业与应用数学学会“几何设计与计算”青年学者奖 2018 年中国科学院数学与系统科学研究院“陈景润未来之星”计划
学术兼职	中国数学会计算机数学专委会秘书长 中国工业与应用数学学会几何设计与计算专委会委员 中国图象图形学学会智能图形专委会委员
学术期刊兼职	

姓名	陈绍示	身份类型	优秀青年骨干
性别	男	年龄	34
最后学位	博士	获得最后学位所在院校	法国巴黎综合理工学校 (计算机科学博士) 中国科学院数学与系统科学研究院(应用数学博士)
任职时间		依托单位职务	

学习及工作经历	2001.9-2005.7 江苏大学 学士 2005.9-2010.12 中科院数学与系统科学研究院 硕士 2007.12-2011.2 中国科学院与巴黎综合理工学校联合培养博士 2011.1 中科院数学与系统科学研究院应用数学博士学位 2012.5 巴黎综合理工学校计算机科学博士学位 导师：李子明（中方）与 Frédéric Chyzak（法方） 2011.2-2011.8 奥地利 Linz 大学符号计算研究所 博士后 2011.8-2013.7 美国北卡罗莱纳州立大学博士后 2013.10-2017.3 中科院数学与系统科学研究院系统所助理研究员 2015.10-2016.8 加拿大菲尔兹数学研究所与滑铁卢大学符号计算研究组 Fields-Ontario Postdoctoral Fellow 2017.3 -至今中科院数学与系统科学研究院系统所副研究员
研究方向	符号计算与组合数学
代表性工作	本人的研究领域是符号计算,计算微分与差分代数,以及在组合数学中的应用(尤其是 Wilf-Zeilberger 理论)。近几年的代表性工作主要包括： 1. 通过刻画混合超几何项的结构,解决了相应 Zeilberger 算法的终止性问题与关于超几何函数的 Wilf-Zeilberger 猜想； 2. 引入了几类特殊函数的约化算法,包括超指数函数,超几何项，代数函数,与 Fuchsian D-有限函数,发展了基于约化算法的计算邻差算子的第四代算法; 3. 基于线性微分与差分算子的奇点消解理论，刻画了邻差算子的阶数与次数的代数关系，并且给出了已有的关于奇点消解的启发性算法的高概率正确性的严格数学证明。 4. 证明了系数具有特殊结构的多变元 D-有限幂级数的有理性定理.
个人荣誉	中国科学院青年创新促进会会员，2018-2022. 中国科学院系统科学研究所 2016 年度“关肇直青年研究奖”,2016. 国际符号与代数计算年会 ISSAC2014“Distinguished Poster Award”，2014. 中国科学院数学与系统科学研究院“2014 年度突出科研成果奖”，2014. 中国科学院数学与系统科学研究院第七届“陈景润未来之星”人才计划，2014—2017.
学术兼职	第 43 届国际符号计算与代数计算会议(ISSAC'18，program committee member) 第 41 届国际符号计算与代数计算会议(ISSAC'16，poster committee chair) 第 39 届国际符号计算与代数计算会议(ISSAC'14，program committee member) 第 38 届国际符号计算与代数计算会议(ISSAC'13，poster committee member) 第 10 届亚洲计算数学会议(ASCM'12，program committee member)

学术期刊兼职	ACM Communications in Computer Algebra 编委 Journal of Symbolic Computation, Guest Editor

身份类型：实验室主任、实验室副主任、学术带头人、优秀青年骨干
此表格可以复制，请自行添加。

3.国际学术机构和国际学术期刊任职情况

序号	姓名	学术组织/期刊名称	职务	任职开始时间	任职结束时间
1.	高小山	ACM SIGSAM Advisory Committee Board	委员	2006	
2.	高小山	ICIAM Member Committee	委员	2016	
3.	刘卓军	System Safety Society	会员	2011	
4.	李子明	ISSAC 指导委员会	委员	2016	2018
5.	支丽红	ACM SIGSAM	副主席	2017	2019
6.	支丽红	Thematic Program on Computer Algebra	委员	2015	
7.	支丽红	Symbolic and Numeric Computation	委员	2004	
8.	支丽红	ISSAC2017 组委会	委员	2017	2017
9.	支丽红	FSCD 2018 组委会	委员	2017	2018
10.	闫振亚	2017 可积系统与偏微分方程国际学术研讨会程序委员会	委员	2017	2017
11.	闫振亚	第 7 届非线性数学物理国际会议暨全国第 14 届孤立子与可积系统研讨会程序委员会	委员	2017	2017
12.	贾晓红	International Conference of Geometric Modeling and Processing 2017 程序委员会	委员	2017	2017
13.	贾晓红	International Conference of Geometric Modeling and Processing 2018 程序委员会	委员	2017	2018
14.	贾晓红	13th International Conference on Artificial Intelligence and Symbolic Computation	宣传主席	2017	2018

15.	程进三	CASC 程序委员会	委员	2017	2017
16.	冯秀涛	CTCIS 2017 程序委员会	委员	2017	2017
17.	陈绍示	ISSAC2018 程序委员会	委员	2017	2018
18.	潘彦斌	ISC 2017 程序委员会	委员	2017	2017
19.	万哲先	《Algebra Colloquium》	主编		
20.	万哲先	《Annals of Combinatorics》	编委		
21.	万哲先	《Discrete Applied Mathematics》	编委		
22.	万哲先	《Finite Fields and Their Applications》	编委		
23.	万哲先	《Journal of Combinatorics, Information and System Sciences》	编委		
24.	高小山	《Journal of Systems Science and Complexity》	主编		
25.	高小山	《Journal of Symbolic Computation》	编委		
26.	高小山	《International Journal of Computers Communications & Control》	编委		

27.	高小山	《Electronic Journal of Mathematics and Technology》	编委		
28.	刘卓军	《The International System Safety Society》	Member		
29.	李洪波	《Journal of Systems Science and Complexity》	编委		
30.	李洪波	《Advances in Applied Clifford Algebras》	编委		
31.	李子明	《Journal of Symbolic Computation》	编委		
32.	支丽红	《Journal of Symbolic Computation》	编委		
33.	支丽红	《Mathematics in Computer Science》	编委		
34.	支丽红	《ACM Communications in Computer Algebra》	编委		
35.	支丽红	《SIAM Journal on Applied Algebra and Geometry》	编委		
36.	支丽红	《Theoretical Computer Science》	特辑编委		

37.	闫振亚	《Plos ONE》	学术编委		
38.	闫振亚	《Sci. Rep》	学术编委		
39.	邓映蒲	《Journal of Systems Science and Complexity》	编委		
40.	张志芳	《Journal of Systems Science and Complexity》	编委		
41.	程进三	《AMS Mathematics Reviews》	编委		
42.	陈绍示	《ACM Communicatons in Computer Algebra》	编委		

三、开放交流与运行管理

1. 对外开放

（访问学者制度建设情况，吸引国际同领域实验室人员到本实验室开展访问学者研究工作和国内外优秀博士毕业生到实验室开展博士后研究工作的情况。

设置开放课题的情况，以及开放课题所取得的重要成果等。）

2017 年，实验室邀请了 100 余位专家学者进行有关数学机械化相关领域的学术报告以及访问交流研究。

实验室目前有 4 位博士后，其中李建伟和沈雨佳分别获得了 2015 年和 2016 年支持“率先行动”联合资助优秀博士后项目以及中国博士后科学基金。

2017 年，实验室设有开放课题 6 项：

1、 杨争峰副教授承担“符号计算程序验证”课题，与实验室成员支丽红研究员在基于符号执行将程序的测试用例生成问题方面开展了合作研究。他将程序测试问题转化为非线性约束求解问题，运用计算实代数几何理论设计高效的误差可控算法，用于求解相应的(半)代数系统的精确解，从而给出能准确满足测试覆盖准则的测试用例。

2、 谢福鼎教授承担“生物学原理的优化算法”课题，与实验室成员王定康研究员在充分讨论的基础上结合高光谱图像的分类问题，进行了具体的算法设计。高光谱数据

处理，特别是高光谱数据的分类问题，一直是遥感领域研究的热点问题之一。高光谱数据的高维特征为这一工作带了很大的困难，不但严重影响了分类精度，更是带来了巨大的运算量。因此开展高光谱数据的降维算法研究十分必要。在典型的高光谱数据将为方法中，我们选择了波段选择方法，因为所选波段可以保持原有波段的物理意义和地学特征。在综合分析了几个优化算法之后，我们确定采用蜂群算法进行波段选择和优化，其中适优化准则采用香浓熵。通过定义新的适应度函数达到选择最优波段的目的。最后，采用五重交叉验证的支持向量机作为分类器。目前该成果正在整理成论文。

3、 顾险峰教授与实验室贾晓红副研究员合作研究“Geometric Interpretation to Generative Learning Model（生成对抗网络模型的几何解释）”，取得了如下成果：用最优传输理论解释了生成对抗网络模型的原理；给出生成对抗网络在机器统计学习中的几个具体应用；给出了隐式网络模型与最优传输模型在具体几何计算问题中的比较效果。

4、 朱佐农教授与实验室闫振亚研究员主要合作交流讨论有关非局域可积系统，通过一些对称变换等，建立已知典型局域可积系统与新的非局域可积系统之间的关系，揭示它们的非线性波之间的联系等。

5、 周子翔教授与实验室闫振亚研究员主要合作交流讨论可积系统的Darboux变换及其应用，包括一维和二维可积系统，探索经典Darboux变换与广义Darboux变换之间的内在联系，分析由广义Darboux变换导出怪波的内在原理等。

6、 张立先与实验室副研究员袁春明合作研究“数控加工中的小线段过渡方法与优化”，基于原有的张立先等人设计的小线段过渡算法,设计了新的计算步骤与方法，使得这一方法可以移植到国产数控系统里。基于这一算法,设计了修调算法，从而使这一算法可以应用到商用数控中．此外,也设计了针对圆弧样条的速度规划与插补的高效计算方法，并将其嵌入到商用数控系统中。

2. 科学传播

（实验室开展科学知识、科学精神和实验室文化的传播情况，向社会公众特别是学生科学传播的情况，以及取得的成效。）

为了让公众更好地认识和了解数学与系统科学，2017年5月20日，中科院数学院举办了主题为“探索塑造未来”的第十三届公众科学日活动，通过科普报告、系统演示、网络多

媒体展示、展板展示等多种形式，向社会公众展示数学与系统科学的魅力，介绍数学和系统科学与国民经济、与人民生活的密切关系，激发公众对数学和系统科学的热爱。来自大、中、小学校和社会各界的 400 多名来访者参与了我院举办此次公众科学日活动。

在南楼二层进行了数学机械化研究成果的系统演示。很多参观者看完后，纷纷感叹数学科学的神奇与伟大，充分激发了自己对探索数学科学奥秘的欲望。

四、依托单位的支持

1.依托单位在人、财、物条件方面的保障和支持

类别	上一年度	本年度	增长数	增长比率
专职管理人员（个）	2	2	0	0
专职技术人员（个）	1	1	0	0
硕士研究生招生（个）	11	12	1	8.3%
博士研究生招生（个）	2	2	0	0
单位配套运行费（万元）	112	104	-8	-7.69%
单位配套设备费（万元）	0	0	0	0
实验室总面积（平米）	1200	1200	0	0
实验室总资产（万元）	399.538	384.3927	-15.1453	-3.94%

2.依托单位给予的其他支持

无

第三部分 人员情况

1. 固定人员名单

序号	姓名	性别	证件类型	证件编号	出生日期	职称等级	实验室职务	所学专业	工作性质	最后学位	学位取得时间	授予单位	进入实验室时间	离开实验室时间	职称名称	研究方向	国别	国籍
1.	吴文俊	男	身份证	110108191905121410	1919.05.12	正高级	名誉主任	数学	研究人员	博士	1949.6	法国斯特拉斯堡大学	2002		院士	数学机械化	国内	中国
2.	万哲先	男	身份证	11010819271107143X	1927.11.07	正高级		数学	研究人员	学士	1948.6	清华大学	2002		院士	代数、编码、有限几何	国内	中国
3.	李邦河	男	身份证	110108194207071413	1942.07.07	正高级	学术委员会主任	数学	研究人员	学士	1965.6	中国科学技术大学	2002		院士	拓扑、代数几何	国内	中国
4.	高小山	男	身份证	11010819631003121X	1963.10.03	正高级	学术委员会副主	应用数学	研究人员	博士	1988.6	中国科学院系统科学研究所	2002		研究员	自动推理、符号计算	国内	中国

							任											
5.	李洪波	男	身份证	110108196803041818	1968.03.04	正高级	实验室主任	应用数学	研究人员	博士	1994.6	北京大学	2002		研究员	自动推理、几何代数	国内	中国
6.	刘卓军	男	身份证	110108195803081479	1958.03.08	正高级		应用数学	研究人员	博士	1988.6	中国科学院系统科学研究所	2002		研究员	信息安全	国内	中国
7.	李子明	男	身份证	110108196206061490	1962.06.06	正高级	实验室副主任	应用数学	研究人员	博士	1996.4	奥地利林茨大学	2002		研究员	符号计算	国内	中国
8.	支丽红	女	身份证	110108196906221846	1969.06.22	正高级	实验室副主任	应用数学	研究人员	博士	1996.6	中国科学院系统科学研究所	2002		研究员	混合计算	国内	中国
9.	韩阳	男	身份证	21031919711029233X	1971.10.29	正高级		基础数学	研究人员	博士	1999.6	德国 Bielefeld Univesity	2003		研究员	代数表示论	国内	中国
10.	王定康	男	身份证	110108196503021874	1965.03.02	正高级		应用数学	研究人员	博士	1993.6	中国科学院系统科学研究所	2002		研究员	符号计算	国内	中国
11.	闫振亚	男	身份证	412825197403078517	1974.03.07	正高		应用数	研究人	博士	2002.5	大连理工大学	2003		研究员	数学物理	国内	中国

						级		学	员									
12.	邓映蒲	男	身份证	420106197105294839	1971.05.29	正高级	实验室副主任	应用数学	研究人员	博士	2002.6	北京大学	2004		研究员	信息安全	国内	中国
13.	冯如勇	男	身份证	352201197806234713	1978.06.23	副高级		应用数学	研究人员	博士	2005.6	中国科学院数学与系统科学研究院	2005		副研究员	符号计算	国内	中国
14.	张志芳	女	身份证	429001198010130423	1980.10.13	副高级		应用数学	研究人员	博士	2007.6	中国科学院数学与系统科学研究院	2007		副研究员	信息安全	国内	中国
15.	袁春明	男	身份证	320222197912082279	1979.12.08	副高级		应用数学	研究人员	博士	2007.6	中国科学院数学与系统科学研究院	2007		副研究员	符号计算	国内	中国
16.	程进三	男	身份证	220104197608121534	1976.08.12	副高级		应用数学	研究人员	博士	2006.6	中国科学院数学与系统科学研究院	2009		副研究员	符号计算	国内	中国
17.	贾晓红	女	身份证	142401198109231425	1981.09.23	副高级		应用数学	研究人员	博士	2009.6	中国科学技术大学	2011		副研究员	计算几何	国内	中国
18.	冯秀涛	男	身份证	610103197808122O1X	1978.08.12	副高级		理论密码学	研究人员	博士	2006.6	中国科学院大学	2012		副研究员	信息安全	国内	中国
19.	陈	男	身	330327198307171576	1983.07.17	副		应	研	博	2011.2	中国科学	2013		副	符号	国	中

	绍示		份证			高级		用数学	究人员	士		院数学与系统科学研究院&巴黎综合理工学校			研究员	计算	内	国
20.	叶科	男	身份证	510105198410181275	1984.10.18	副高级		应用数学	研究人员	博士	2012.8	美国德克萨斯农工大学	2017		副研究员	应用代数几何	国内	中国
21.	潘彦斌	男	身份证	131026198204021015	1982.04.02	中级		应用数学	研究人员	博士	2010.6	中国科学院数学与系统科学研究院	2010		所聘副研	信息安全	国内	中国
22.	李博	男	身份证	420106198209253278	1982.09.25	中级		应用数学	研究人员	博士	2010.6	中国科学院数学与系统科学研究院	2012		所聘副研	生物数学	国内	中国
23.	李伟	女	身份证	37132119850912142X	1985.09.12	中级		应用数学	研究人员	博士	2012.6	中国科学院数学与系统科学研究院	2012		所聘副研	微分代数几何	国内	中国
24.	吴天骄	男	身份证	11010819590922145X	1959.09.22	中级		自动控制	技术人员	本科	1988.6	北京广播电视大学	2006		工程师		国内	中国
25.	周代珍	女	身份证	11010819650306142X	1965.03.06	中级		经济管理	管理人员	本科	2006.12	中共中央党校	2002		秘书		国内	中国
26.	李佳	女	身份证	140107198412134521	1984.12.13	中级		通信与信息	管理人员	硕士	2010.4	西北工业大学	2012		学术秘书		国内	中国

								系统										

固定人员：指经过核定的属于实验室编制的人员。不包括在读研究生。
证件类型：只能是身份证、军官证、护照。
出生日期：通过身份证号码读取，格式为“年-月-日”；无身份证号码的，可以手动填写。
职称等级：正高级；副高级；中级；初级；其他。
实验室职务：实验室主任、实验室副主任，实验室秘书、其他。
工作性质：研究人员、技术人员、管理人员。
研究人员：指承担研究课题并在实验室主要从事研究工作的固定人员；
技术人员：指主要从事技术性工作的固定人员；
管理人员：指专职负责管理工作的固定人员，主要从事研究工作的兼职管理人员应计入研究人员范围。
最后学位：博士、硕士、学士、其他。
学位取得时间：填写格式为：“年-月-日”，（注意，年月日之间的分隔用减号“-”，excel 单元格格式设置成文本格式）。
研究方向：只填写研究方向的序号。研究人员在实验室的研究方向应与实验室研究方向一致。技术和管理人员可按实际情况填写。
国别：国内、国外。

2.流动人员名单

序号	姓名	性别	出生日期	职称等级	所学专业	最后学位	学位取得时间	授予单位	进入实验室时间	离开实验室时间	工作单位	职称名称	国别	国籍	是否为本实验室博士后
1.	李建伟	男	1987.10.01	中级	基础数学	博士	2015.6	清华大学	2015.7		中国科学院数学与系统科学研究院		国内	中国	是
2.	林望	男	1982.09.04	副高级	计算机应用技术	博士	2013.6	华东师范大学	2015.7		温州大学	副教授	国内	中国	是

3.	邵长鹏	男	1989.01.11	中级	应用数学	博士	2016.6	中国科学院数学与系统科学研究院	2016.7		中国科学院数学与系统科学研究院		国内	中国	是
4.	沈雨佳	男	1987.02.03	中级	流体力学	博士	2016.6	北京航空航天大学	2016.7		中国科学院数学与系统科学研究院		国内	中国	是
5.	谢福鼎	男	1965.08.26	正高级	计算数学	博士	2003.6	大连理工大学	2017.11.6	2017.12.5	辽宁师范大学	教授	国内	中国	否
6.	杨争峰	男	1980.11.13	副高级	应用数学	博士	2006.6	中国科学院数学与系统科学研究院	2017.2.10	2017.3.10	华东师范大学	副教授	国内	中国	否
7.	沈敏捷	男	1993.10.23	学生	信息与计算科学	本科	2015.6	华东师范大学	2017.2.10	2017.3.5	华东师范大学		国内	中国	否

流动人员：指在本实验室做博士后以及编制不在实验室、到实验室从事合作研究或进行开放课题研究的人员，不包括临时聘请的仪器设备维修人员、来室使用仪器但不参加实验室研究的人员及在读研究生等。

3.实验室研究单元

序号	研究单元	研究方向	学术带头人	其它固定人员名单
1	数学机械化研究中心	数学机械化理论	吴文俊、李邦河、高小山、李洪波、李子明、支丽红、王定康、闫振亚	冯如勇、袁春明、程进三、贾晓红、陈绍示、李　伟、叶　科
2	信息安全研究中心	信息安全的数学理论	万哲先、刘卓军、韩　阳、邓映蒲	张志芳、冯秀涛、潘彦斌、李　博

研究方向：与第一部分实验室基本情况列表中的研究方向对应，填写研究方向序号。

4.重要人才情况

	中国科学院院士	中国工程院院士	杰青	优青	千人计划			长江学者	百人计划	万人计划		
					长期(A类)	短期(B类)	青年千人			杰出人才	领军人才	青年拔尖人才
姓名	吴文俊		高小山				叶科		高小山			
	万哲先		李洪波						李洪波			
	李邦河											
数量	3		2				1		2			

请依次列出相应的固定人员姓名，合计处列出合计的人数。

千人计划：千人计划包括创新型和创业型两种人才项目，此处只统计创新型人才项目。

5.基金委创新研究群体

序号	研究方向	学术带头人	参加人员	获批年份
1	数学机械化方法及其在信息技术中的应用	高小山	李洪波、孙笑涛、李子明、刘卓军、王定康、支丽红、闫振亚、冯如勇、袁春明、程进三、黄雷、李伟等	2009-2011 2012-2014

学术带头人：要求是本实验室固定人员。

6. 研究生培养情况

在读硕士一览表

序号	姓名	出生年月	导师姓名	生源校	入学时间	获奖	获奖	获奖
1.	刘珍	1994.10	潘彦斌	湖北大学	2016.09			
2.	马鸿宇	1993.10	袁春明	山西大学	2016.09			
3.	张文剑	1994.09	程进三	湘潭大学	2016.09			
4.	郭婧	1993.08	李子明	湖南大学	2016.09			
5.	骆丽夏	1993.11	邓映蒲	中山大学	2016.09			
6.	史帅	1991.04	李洪波	重庆理工大学	2016.09			
7.	赵明阳	1993.02	贾晓红	河南科技大学	2016.09			
8.	王贺松	1990.11	王定康	南阳师范学院	2016.09			
9.	王丽	1992.12	闫振亚	中国矿业大学	2016.09			
10.	葛京通	1994.12	支丽红	南京师范大学	2016.09			
11.	李爽	1994.10	李邦河	山东师范大学	2016.09			
12.	杜丽欣	1995.01	陈绍示	南方科技大学	2017.09			
13.	傅蕾	1995.07	李伟	苏州大学	2017.09			
14.	秦璐	1994.10	刘卓军	北京大学	2017.09			
15.	吴澄冉	1995.06	李洪波	山东大学	2017.09			
16.	翁为方	1995.08	闫振亚	武汉理工大学	2017.09			
17.	闫斯卓	1995.10	支丽红	西安交通大学	2017.09			
18.	杨润河	1995.02	王定康	北京理工大学	2017.09			
19.	杨小龙	1995.07	贾晓红	西北工业大学	2017.09			
20.	王路	1994.09	张志芳	北京科技大学	2017.09			
21.	杨照民	1995.09	潘彦斌	中山大学	2017.09			
22.	周丽阳	1995.02	张志芳	南京师范大学	2017.09			
23.	朱熠铭	1994.12	潘彦斌	中山大学	2017.09			

导师姓名：要求是本实验室固定人员。

生源校：生源是指进入该实验室之前的学习单位。例如，张三为在读硕士研究生，其本科毕业院校为北京大学，则此处生源填写北京大学。

获奖：院百篇优博、院长特别奖、院长优秀奖。

在读博士一览表

序号	姓名	出生年月	导师姓名	生源校	入学时间	获奖	获奖	获奖
1.	陈　勇	1990.07	闫振亚	河南理工大学	2013.09			
2.	宓振鹏	1990.11	高小山，袁春明	山东师范大学	2013.09			
3.	白　剑	1992.07	王定康	南开大学	2013.09			
4.	杨志红	1991.12	支丽红	中南大学	2013.09			
5.	李秋萍	1989.09	刘卓军	吉林大学	2013.09			
6.	窦孝杰	1989.08	程进三	郑州大学	2013.09			
7.	付仕辉	1988.07	邓映蒲	四川大学	2013.09	院长优秀奖		
8.	周义满	1990.12	韩　阳	电子科技大学	2013.09			
9.	黄巧龙	1990.12	高小山	中国科学技术大学	2013.09			
10.	杜　昊	1993.01	李子明	北京航空航天大学	2014.09			
11.	胡又壬	1992.04.	高小山	四川大学	2014.09			
12.	鲁东	1991.09	王定康	西南交通大学	2014.09			
13.	张国强	1990.11	闫振亚	曲阜师范大学	2014.09			
14.	李彰	1991.12	李洪波	中国科学技术大学	2014.09			
15.	徐敬可	1990.08	张志芳	山东农业大学	2014.09			
16.	李昊宇	1990.10	邓映蒲	武汉大学	2014.09			
17.	陈俣翱	1993.8	高小山	中国科学技术大学	2015.09			
18.	陈淑延	1992.9	闫振亚	福建师范大学	2015.09			
19.	姚姗姗	1991.03	支丽红，贾晓红	山东师范大学	2015.09			
20.	何笑鸥	1990.10	刘卓军	北京大学	2015.09			
21.	冯爽	1992.02	李子明，冯如勇	郑州大学	2015.09			
22.	李阳	1994.02	李洪波	北京科技大学	2015.09			
23.	肖方慧	1991.06	王定康	湖南师范大学	2015.09			
24.	文钧屹	1993.10	程进三	吉林大学	2015.09			
25.	程恒喆	1992.08	冯秀涛	曲阜师范大学	2015.09			

26.	谢天元	1992.01	邓映蒲、潘彦斌	中山大学	2015.09			
27.	刘欣	1993.5	韩　阳	厦门大学	2015.09			
28.	王凯	1993.09	韩　阳	四川大学	2015.09			
29.	张雅倩	1993.07	张志芳	东北大学	2015.09			
30.	王建华	1993.09	刘卓军	大连理工大学	2016.09			
31.	朱超超	1993.10	陈绍示	济南大学	2016.09			
32.	赵　宸	1995.09	高小山	中山大学	2017.09			
33.	王永兴	1995.10	邓映蒲	武汉大学	2017.09			

当年毕业研究生一览表

序号	姓名	学历	导师姓名	毕业去向	获奖
1.	荆瑞娟	博士	高小山	加拿大西安大略大学博士后	
2.	王　杰	博士	高小山	北京大学博士后	
3.	郝志伟	博士	支丽红	华为技术有限公司	
4.	温子超	博士	闫振亚	华盛顿大学圣路易斯大学博士后	院长特别奖
5.	李　昕	博士	闫振亚	常熟理工学院	
6.	王立波	博士	刘卓军	暨南大学	
7.	杨江帅	博士	邓映蒲	中国电子信息产业集团有限公司第六研究所	
8.	王　慧	博士	邓映蒲	北京握奇数据股份有限公司	
9.	廖茂东	博士	邓映蒲	61786 部队	
10.	张凝鹏	博士	韩　阳	华为技术有限公司	
11.	李加宁	博士	邓映蒲	中国科学技术大学博士后	
12.	齐嘉悦	硕士	高小山	奥地利林茨大学博士	
13.	姜文嵘	硕士	支丽红	国家电网	
14.	郑　策	硕士	韩　阳	清华大学附属中学	

毕业去向：填写学习/工作单位名称

第四部分 承担任务及经费

1. 承担任务一览表

序号	项目名称	项目来源	项目类别	开始时间	结束时间	总经费(万元)	本年度实到经费（万元）	负责人	参与类型
1.	量子基础算法及其在密码分析中的应用	其他	科技委项目	2017	2017	410	410	李洪波	主要负责
2.	初等数学问题求解关键技术及系统	科技部	“863”计划项目课题	2015	2017	70	30.49	黄雷	参与
3.	数学定理的机器证明和数学证明的验证补充	中国科学院	前沿科学重点研究项目	2017	2022	100	10	李洪波	主要负责
4.	CXJJ-17-M142	中科院		2017	2019	60	30	冯秀涛	主要负责
5.	数学化设计制造中的数学机械化方法	中国科学院	国家数学交叉中心	2017	2017	61	61	李洪波	主要负责
6.	微分差分方程符号计算与机器证明	中国科学院	国家数学交叉中心	2017	2017	37	37	李子明	主要负责
7.	信息安全和密码体系	中国科学院	国家数学交叉中心	2017	2017	31.5	31.5	邓映蒲	主要负责
8.	面向 E 量级系统的并行算法与应用支撑技术	科技部	国家重点研发计划	2016	2018	30	18	支丽红	参与
9.	基于签名的 Groebner 基算法及其应用	国家自然科学基金委	面上项目	2014	2017	50	0	王定康	主要负责
10.	素数判定与整数分解	国家自然科学基金委	面上项目	2015	2018	60	15	邓映蒲	主要负责
11.	（半）代数系统的几何结构分析的高效算法及其应用	国家自然科学基金委	面上项目	2015	2018	65	16.25	程进三	主要负责
12.	Hochschild（上）同调及其在代数表示论中的应用	国家自然科学基金委	面上项目	2016	2019	52.68	13.5	韩阳	主要负责

13.	凸代数几何中的若干问题研究	国家自然科学基金委	面上项目	2016	2019	53.8	13.5	支丽红	主要负责
14.	PT-对称的非线性波方程的波结构及其稳定性分析研究	国家自然科学基金委	面上项目	2016	2019	59.7	15	闫振亚	主要负责
15.	流密码算法设计与分析机械化方法研究	国家自然科学基金委	面上项目	2016	2019	78	19.5	冯秀涛	主要负责
16.	格上最短向量问题的求解算法研究	国家自然科学基金委	面上项目	2016	2019	77.2	19.5	潘彦斌	主要负责
17.	几何定理机器证明的代数方法的等价性与完全性	国家自然科学基金委	面上项目	2017	2020	48	24	李洪波	主要负责
18.	Wilf-Zeilberger理论的算法设计，复杂度分析及其应用	国家自然科学基金委	青年项目	2016	2018	19.96	6.8	陈绍示	主要负责
19.	Zeilberger方法在含参微分伽罗瓦理论中的应用	教育部	留学回国启动经费	2015	2018	3	0	陈绍示	主要负责
20.	重大交叉学科前沿发展路线图战略研究	中国科学院	其他	2017	2017	100	100	高小山	主要负责
21.	中国科学院青年创新促进会	中国科学院	其他	2014	2017	50	20	闫振亚	主要负责
22.	中国科学院青年创新促进会	中国科学院	其他	2014	2017	50	20	冯如勇	主要负责
23.	中国科学院青年创新促进会	中国科学院	其他	2015	2018	60	20	袁春明	主要负责
24.	城市综合评价模型研究	中国科学院	STS计划	2015	2017	35	15	刘卓军	主要负责
25.	一种基于格的公钥密码体制的设计	中国电子科技集团公司第三十研究所	其他	2015	2017	14	0	潘彦斌	主要负责
26.	格基约化与提取	中国科学院信息工程	开放课题	2016	2017	10	5	潘彦斌	主要负责

		研究所国家重点实验室							
27.	序列密码设计与分析新进展咨询研究	中国人民解放军61569部队	其他	2017	2018	28.59	14	冯秀涛	主要负责
28.	区块链抗量子加密技术研究	北京太一云科技有限公司	其他	2017	2019	60	24	冯秀涛	主要负责
29.	虚拟现实环境中的碰撞检测理论研究	北京控制电子技术研究所	其他	2017	2017	4	2	贾晓红	主要负责
30.	三轴数控系统加工算法优化试验与配套应用项目	广西玉柴机器股份有限公司	其他	2017	2018	27	17.88	袁春明	主要负责
31.	2015年支持“率先行动”联合资助优秀博士后项目	中国科学院	其他	2016	2017	10	0	李建伟	主要负责
32.	2016年支持“率先行动”联合资助优秀博士后项目	中国科学院	其他	2017	2018	10	10	沈雨佳	主要负责
33.	中国博士后科学基金	中国博士后科学基金会	其他	2016	2017	5	0	李建伟	主要负责
34.	中国博士后科学基金	中国博士后科学基金会	其他	2016	2017	5	0	沈雨佳	主要负责
合计	\	\	\	\	\		1018.92	\	\

承担任务只包括项目、课题，不统计子课题。
项目来源：科技部、国家自然科学基金委、中国科学院、横向项目、其他；
项目类别：请填写具体的项目类别，如重点研发计划、面上项目等；
参与类型：主要负责、参与。

2. 国际合作项目一览表

序号	项目名称	合作国别	合作单位	开始时间	结束时间	总经费(万元)	本年实到经费（万元）	负责人
1								
2								
合计	\	\	\	\	\			\

国际合作项目指双方单位正式签订协议书的国际合作科研项目。

合作单位：应为合作国家的单位。

第五部分 研究成果

1. 获奖情况

序号	成果名称	级别	类别	等级	完成人	排名
1.	数学与量子物理效应创新交叉团队	其他	中科院 2017 年度创新交叉团队	集体	闫振亚	
2.		其他	中科院百人计划 C	其他	叶　科	
3.		其他	中科院优秀青年人才	其他	叶　科	
4.		其他	中国工业与应用数学学会“几何设计与计算”青年学者奖	其他	贾晓红	
5.		其他	中科院数学院第十届“ 陈景润未来之星 ”	其他	贾晓红	
6.		其他	吴文俊计算机数学青年学者奖	其他	冯如勇	
7.		其他	2017 年中国高被引学者(爱思唯尔发布)	其他	高小山	
8.		其他	2017 年中国高被引学者(爱思唯尔发布)	其他	闫振亚	
9.		其他	2017 年中科院优秀导师奖	其他	闫振亚	

级别：国家级、省部级、其他
类别：最高科学技术奖、自然科学奖、技术发明奖、科学技术进步奖
等级：特等、集体、一等、二等、其他
排名：阿拉伯数字

2. 发表论文一览表

序号	论文名称	期刊名称	卷、期、页	收录类型	是否为1区论文	作者	通讯作者（固定人员）	通讯作者（非固定人员）	完成情况
1.	Power Series with Coefficients from a Finite Set	Journal of Combinatorial Theory	Series A., 151, 241-253, 2017	SCI收录	否	Jason P. Bell, Shaoshi Chen	Shaoshi Chen		非第一完成人(非独立完成)
2.	Some Open Problems Related to Creative Telescoping	Journal of Systems Science and Complexity	30(1), 154-172, 2017	SCI收录	否	Shaoshi Chen, Manuel Kauers	Shaoshi Chen		第一完成人(非独立完成)
3.	Certifying Simple Zeros of Over-Determined Polynomial Systems	CASC	66-76, 2017	EI收录	否	Jin-San Cheng, Xiaojie Dou	Jin-San Cheng		第一完成人(非独立完成)
4.	Algorithm for computing the factor ring of an ideal in Dedekind domain with finite rank	Science China: Mathematics	3 (1), 1-14, 2017	SCI收录	否	Dandan Huang, Yingpu Deng	Yingpu Deng		非第一完成人(非独立完成)

5.	Combinatorial Sums $\sum_{k\equiv r(\mbox{mod } m)}{n\choose k}a^k$ and Lucas Quotients	Moscow Journal of Combinatorics and Number Theory	7(4), 2017	SCI 收录	否	Jiangshuai Yang, Yingpu Deng	Yingpu Deng		非第一完成人(非独立完成)
6.	Nonexistence of two classes of generalized bent functions	Designs, Codes and Cryptography	85(3), 471-482,2017	SCI 收录	否	Jianing Li, Yingpu Deng	Yingpu Deng		非第一完成人(非独立完成)
7.	On the integral representation of binary quadratic forms and the Artin condition	Tokyo Journal of Mathematics	Accepted	SCI 收录	否	Chang Lv, Junchao Shentu, Yingpu Deng	Yingpu Deng		非第一完成人(非独立完成)
8.	On the computation of the Galois group of linear difference equations	Mathematics of Computation	DOI: 10.1090/mcom/3232	SCI 收录	否	Ruyong Feng	Ruyong Feng		独立完成
9.	Differentially 4-Uniform Permutations with the Best Known Nonlinearity from Butterflies	IACR Transactions on Symmetric Cryptology	2017(2), 228-249, 2017	EI 收录	否	Shihui Fu, Xiutao Feng, Baofeng Wu	Xiutao Feng		非第一完成人(非独立完成)
10.	Fault Attack on the Authenticated Cipher ACORN v2	Security and Communication Networks	https://doi.org/10.1155/2017/3834685	SCI 收录	否	Xiaojuan Zhang, Xiutao Feng, Dongdai Lin	Xiutao Feng		非第一完成人(非独立完成)

11.	The adjacency graphs of a class of LFSRs and their applications	Chinese Journal of Electronics	Accepted	SCI 收录	否	Wang Hui, Xiutao Feng	Xiutao Feng		非第一完成人(非独立完成)
12.	一类模加差分方程系统解个数的期望与方差	中国科学: 数学	47(11), 1545- 1556, 2017	其他	否	冯秀涛, 张凡, 黄慎	冯秀涛		第一完成人(非独立完成)
13.	认证加密算法 FASER 的安全性分析	密码学报	2017 年 9 月接收	其他	否	冯秀涛, 张凡	冯秀涛		第一完成人(非独立完成)
14.	A triangular decomposition algorithm for differential polynomial systems with elementary computation complexity	Journal of Systems Science and Complexity	30(2), 464-483, 2017	SCI 收录	否	W. Zhu, X.S. Gao	X.S. Gao		非第一完成人(非独立完成)
15.	An Efficient Stochastic Approach for Robust Time-Optimal Trajectory Planning of Robotic Manipulators Under Limited Actuation	Robotica	35(12), 2400-241, 2017	SCI 收录	否	M.Y. Zhao, X.S. Gao	X.S. Gao		非第一完成人(非独立完成)

16.	Binomial difference ideals	Journal of Symbolic Computation	80, 665-706, 2017	SCI 收录	否	X.S. Gao, Z. Huang, C.M. Yuan	X.S. Gao		第一完成人(非独立完成)
17.	Characteristic Set Method for Laurent Differential Polynomial Systems	Proc. CASC'17	LNCS 10490, 183-195, 2017	EI 收录	否	Y. Hu, X.S. Gao	X.S. Gao		非第一完成人(非独立完成)
18.	Criteria for Finite Difference Groebner Bases of Normal Binomial Difference Ideals	Prof. ISSAC'17	93-100, 2017	EI 收录	否	Y.AChen , X.S. Gao	X.S. Gao		非第一完成人(非独立完成)
19.	Linear programming and windowing based feedrate optimization for spline toolpaths	CIRP Annals - Manufacturing Technology	66, 393-396, 2017	SCI 收录	否	K. Erkorkmaz, Q.G. Chen, M.Y. Zhao, X. Beudaert, X.S. Gao	X.S. Gao		非第一完成人(非独立完成)
20.	Minimum time corner transition algorithm with confined feedrate and axial acceleration for nc machining along linear tool path	Int J Adv Manuf Technol	89, 941-956, 2017	SCI 收录	否	Q. Zhang, X.S. Gao, H.B. Li, M.Y. Zhao	X.S. Gao		非第一完成人(非独立完成)

21.	Sparse Polynomial Interpolation with Finitely Many Values for the Coefficients	Proc. CASC'17	LNCS 10490, 196-209, 2017	EI 收录	否	Q.L. Huang, X.S. Gao	X.S. Gao		非第一完成人(非独立完成)
22.	Sparse Rational Function Interpolation with Finitely Many Values for the Coefficients	Mathematical Aspects of Computer and Information Sciences	LNCS 10693, 227-242, 2017	EI 收录	否	Q.L. Huang, X.S. Gao	X.S. Gao		非第一完成人(非独立完成)
23.	Toric Difference Variety	Journal of Systems Science and Complexity	30(1), 173-195, 2017	SCI 收录	否	X.S. Gao, Z. Huang, J. Wang, C.M. Yuan	X.S. Gao		第一完成人(非独立完成)
24.	Quaternion Rational Surfaces	Journal of Commutative Algebra	to appear. https://projecteuclid.org/euclid.jca/1507276950	SCI 收录	否	J. Hoffman, X. Jia, H. Wang	X. Jia		非第一完成人(非独立完成)
25.	Behavioral heterogeneity and financial markets: Locked/crossed quotes under informationally efficient pricing	Cogent Economics & Finance	5(1), 1384524, 2017	其他	否	Youzong Xu, Bo Li	Bo Li		非第一完成人(非独立完成)

26.	Boolean Gossiping Networks	IEEE/ACM Transactions on Networking	Accepted	SCI 收录	否	Bo Li, Junfeng Wu, Hongsheng Qi, A. Proutiere, Guodong Shi	Bo Li		第一完成人(非独立完成)
27.	Reaching Agreement in Quantum Hybrid Networks	Scientific Reports	7, 5989, 2017	SCI 收录	否	Guodong Shi, Bo Li, Zibo Miao, Peter M. Dower, Matthew R. James	Bo Li		非第一完成人(非独立完成)
28.	Automated Geometric Reasoning with Geometric Algebra:Theory and Practice	Proc. ISSAC 2017	7-8, 2017	EI 收录	否	H. Li	H. Li		独立完成
29.	Riemann Tensor Polynomial Canonicalization by Graph Algebra	Extension. Proc. ISSAC 2017	269-276, 2017	EI 收录	否	H. Li, Z. Li, Y. Li.	H. Li		第一完成人(非独立完成)
30.	Differential Chow Varieties Exist	J. Lond. Math. Soc.	95(2), 128-156, 2017	SCI 收录	否	J. Freitag, W. Li, T. Scanlon	W. Li		非第一完成人(非独立完成)
31.	A q-analogue of the modified Abraomov-Petkovsek reduction	Proc. Of WWCA	Accepted	其他	否	Hao Du, Hui Huang, Ziming Li	Ziming Li		非第一完成人(非独立完成)

32.	Further results on permutation polynomials of some form over finite	Finite Fields and Their Applications	44, 92-112, 2017	SCI 收录	否	Wang Libo, Wu Baofeng, Liu Zhuojun	Liu Zhuojun		非第一完成人(非独立完成)
33.	The Search Successive Minima Problem isEquivalent to Its Optimization Version	Proc. of WISA 2017	Springer, LNCS, 2017	EI 收录	否	Haoyu Li, Yanbin Pan	Yanbin Pan		非第一完成人(非独立完成)
34.	A New Algorithm for General Factorizations of Multivariate Polynomial Matrices	Proc. ISSAC 2017	277-284, 2017	EI 收录	否	Dong Lu, XiaodongMa, Dingkang Wang	Dingkang Wang		非第一完成人(非独立完成)
35.	A New Algorithm for Computing the ExtendedHensel Construction of Multivariate Polynomials	Journal of Systems Science and Complexity	Accepted	SCI 收录	否	Dong Lu, Yao Sun, Dingkang Wang	Dingkang Wang		非第一完成人(非独立完成)
36.	Automated Reducible Geometric Theorem Proving and Discovery by Gröbner Basis	MethodJournal of Automated Reasoning	59, 331-344, 2017	SCI 收录	否	JieZhou, Dingkang Wang, Yao Sun	Dingkang Wang		非第一完成人(非独立完成)
37.	On Checking Linear Dependence of Parametric Vectors	ICIC 2017: Intelligent Computing Theories and Application	LNCS 10362, 188-196, 2017	EI 收录	否	Xiaodong Ma, Yao Sun, Dingkang Wang, YushanXue	Dingkang Wang		非第一完成人(非独立完成)

38.	Preimage Attacks on the Round-reduced KECCAK with Cross-linear Structures	FSE2018	Accepted	EI 收录	否	Ting Li, Yao Sun, Maodong Liao, Dingkang Wang	Dingkang Wang		非第一完成人(非独立完成)
39.	The Generalized RabinowitschTrick	SpringerPROMS	198, 219-229, 2017	EI 收录	否	Deepak Kapur, Yao Sun, Dingkang Wang, Jie Zhou	Dingkang Wang		非第一完成人(非独立完成)
40.	The Lightest 4 × 4 MDS Matrices over GL(4,F2)	SCIENCE CHINA Information Sciences	Accepted	SCI 收录	否	JianBai, Ting Li, Yao Sun, Dingkang Wang, Dongdai Li	Dingkang Wang		非第一完成人(非独立完成)
41.	An initial-boundary value problem for the integrable spin-1 Gross-Pitaevskii equationswith a 4×4 Lax pair on the half-line	Chaos	27, 053117, 2017	SCI 收录	否	Z. Yan	Z. Yan		独立完成
42.	Higher-order rational solitons and rogue-like wave solutions of the (2 + 1)-dimensional nonlinear fluid mechanicsequations	Commun Nonlinear Sci Numer Simulat	43, 311, 2017	SCI 收录	否	X. Wen, Z. Yan	Z. Yan		非第一完成人(非独立完成)

43.	Modulational instability, beak-shapedrogue waves, multi-dark-dark solitons anddynamics in pair-transition-coupled nonlinearSchrödinger equations	Proc.R.Soc. London	A473,20170243, 2017	SCI 收录	否	G. Zhang, Z. Yan, W.-Y Wen	Z. Yan		非第一完成人(非独立完成)
44.	Novel higher-order rational solitons and dynamics of thedefocusing integrable nonlocal nonlinear Schrödinger equation viathe determinants	Appl. Math. Lett	69, 113, 2017	SCI 收录	否	G. Zhang, Z. Yan, Y. Chen	Z. Yan		非第一完成人(非独立完成)
45.	Solitons and their stability in the nonlocal nonlinear Schrödinger equation with PT-symmetric potentials	Chaos	27, 053105, 2017	SCI 收录	否	Z. Wen, Z. Yan	Z. Yan		非第一完成人(非独立完成)
46.	Stable parity-time-symmetric nonlinear modes and excitations in a derivative nonlinearSchrodinger equation	Phys. Rev. E	95, 012205, 2017	SCI 收录	否	Y. Chen, Z. Yan	Z. Yan		非第一完成人(非独立完成)

47.	Stable solitons in the 1D and 2D generalizednonlinear Schrödinger equations with theperiodic effective mass and PT –symmetricpotentials	Ann. Phys.	386, 44, 2017	SCI 收录	否	Y. Chen, Z. Yan	Z. Yan		非第一完成人(非独立完成)
48.	The nonlinear Schrodinger equation with generalized nonlinearities and PT -symmetric potentials: Stable solitons, interactions, and excitations	Chaos	27, 073114, 2017	SCI 收录	否	Z. Yan, Y. Chen,	Z. Yan		第一完成人(非独立完成)
49.	Cohomology of Cryo-Electron microscopy	SIAM journal on Applied Geometry and Algebra	1-1, 507-535, 2017	SCI 收录	否	Ke Ye, Lek-Heng Lim	Ke Ye		第一完成人(非独立完成)
50.	Inverse tensor eigenvalue problem	Communications in Mathematical Sciences	15-6, 1627-1649, 2017	SCI 收录	否	Ke Ye, Shenglong Hu	Ke Ye		第一完成人(非独立完成)
51.	New classes of matrix decompositions	Linear Algebra and its Applications	514, 47-81, 2017	SCI 收录	否	Ke Ye	Ke Ye		独立完成

52.	A Modular Algorithm to Compute the Generalized Hermite Normal Form for Z[x]-Lattices	Journal of Symbolic Computation	81, 97-118, 2017	SCI 收录	否	R.J. Jing, C.M. Yuan	C.M. Yuan		非第一完成人(非独立完成)
53.	Tool orientation optimization for 5-axis machining with C-space method	Int J Adv Manuf Technol	88(5), 1243-1255, 2017	SCI 收录	否	Z. Mi, C.M. Yuan, X. Ma, L.Y. Shen	C.M. Yuan		非第一完成人(非独立完成)
54.	Bounds and constructions for linear locally repairable codes over binary fields	ISIT 2017	2033-2037, 2017	EI 收录	否	Anyu Wang, Zhifang Zhang, Dongdai Lin	Zhifang Zhang		非第一完成人(非独立完成)
55.	构造小域上的最优局部修复码	中国科学:数学	47(11), 1607-1614, 2017	其他	否	张志芳, 徐敬可, 刘木兰	张志芳		第一完成人(非独立完成)
56.	Computing Multiple Zeros of Polynomial Systems: Case of Breadth One	Proc. International Workshop on Computer Algebra in Scientific Computing	392-405, 2017	EI 收录	否	Lihong Zhi	Lihong Zhi		独立完成

57.	Polynomial time interactive proofs for linear algebra with exponential matrix dimensions and scalars given by polynomial time circuits	Proc. 2017 ACM Internat. Symp. Symbolic Algebraic Comput.	125-132, 2017	EI 收录	否	Jean-Guillaume Dumas, Erich L. Kaltofen, Gilles Villard, Lihong Zhi	Lihong Zhi		非第一完成人(非独立完成)

收录类型：SCI 收录、EI 收录、ISTP 收录、ISR 收录、其他。
作者：所有作者，以出版物排序为准。
完成情况：独立完成、第一完成人(非独立完成)、非第一完成人(非独立完成)。

3. 其他成果一览表

序号	类别	成果名称	编号	完成人（固定人员）	完成人（非固定人员）	完成情况	授权日期	国别
1	发明专利	一种基于多项式约化的初等数列问题自动求解技术	2017104562482	李洪波	黄雷、邵长鹏	申请	2017.6.16	国内

类别：发明专利、新药证书、软件证书、国家标准、规范、数据库、农业新品种、其他，“其他”为等同于发明专利的成果。
编号：专利指当年授权的发明专利，实用新型专利不在统计范围内，国内外同内容的发明专利不得重复填报。
国别：国内、国外。

4. 出版专著一览表

序号	著作名称	类别	作者	出版单位	出版年份
1	Rogue Waves: Mathematical Theory and Applications in Physics.	国外	B. Guo, L. Tian, Z. Yan, L. Ling, Y. Wang	Walter de Gruyter GmbH & Co KG	2017
2	Theoretical Computer Science.	国外	Jan Verschelde, Stephen M. Watt, Lihong Zhi	Special issue on Symbolic-Numeric Computation,1-231	2017

类别：国内、国外。

第六部分 开放交流与运行管理

1. 举办的学术会议一览表

序号	会议名称	会议类型	主办/承办单位名称	会议主席	会议日期	会议地址	参加人数
	量子计算与密码分析研讨会		中国科学院数学机械化实验室	李洪波	2017-04-20	中科院数学院	80
	第二届组合数学与符号计算研讨会		中国科学院数学机械化实验室	冯如勇，陈绍示	2017-06-23 2017-06-25	中科院数学院	80
	张量与多项式优化研讨会		中国科学院数学机械化实验室	支丽红	2017-07-07 2017-07-09	西郊宾馆	35
	科学计算中的计算机代数国际会议（CASC2017）	全球性会议	中国科学院数学机械化实验室	高小山	2017-09-18 2017-09-22	中科院数学院	65
	第九届全国计算机数学学术会议（CM2017）	全国性	中国数学会计算机数学专业委员会/湖南科技大学和中国科学院数学机械化实验室	刘金旺	2017-11-19 2017-11-21	湖南湘潭	170
	量子计算与密码分析国际会议		华罗庚数学中心/中国科学院数学机械化实验室	李洪波，王小云	2017-11-01 2017-11-03	中科院数学院	140
	量子计算、量子信息、量子密码冬季学校		华罗庚数学中心/中国科学院数学机械化实验室		2017-11-06 2017-11-10	中科院数学院	120
	可积系统与数学物理相关问题学术论坛		华罗庚数学中心/中国科学院数学机械化实验室		2017-12-09 2017-12-11	中科院数学院	

会议类型：全国性、双边性、区域性、全球性。
全国性会议：是指由国家学术协会组织的，全国性的学术会议
双边性会议：特指由两个国家参加的学术会议
区域性会议：特指在某一地区的两个以上的国家召开的学术会议
全球性会议：是指定期举行的、至少 5 个国家参加、参会的国外人数比例不低于 40%的学术会议 ）
会议时间：填写格式为“-年-月-日”

2. 参加的学术会议一览表

序号	报告名称	报告人	会议名称	地点	时间
1.	Some open problems related to creative telescoping	陈绍示	国际微分代数及其相关领域	奥地利	2017.9

2.	Power series with coefficients from a finite set	陈绍示	Lattice walks at the Interface of Algebra, Analysis and Combinatorics	加拿大	2017.9
3.	D-finite functions: rationality and singularity analysis	陈绍示	第九届全国计算机数学学术会议	湘潭	2017.10
4.	Real solving of Bivariate equation systems	程进三	SIAM conference on Algebraic Geometry	美国	2017.7
5.	Certifying Simple Zeros of Over-Determined Polynomial Systems	程进三	Computer Algebra in Scientific Computing(CASC2017)	北京	2017. 9
6.	Polynomial systems solving	程进三	第九届全国计算机数学学术会议	湘潭	2017.10
7.	Certifying simple zeros of over-determined polynomial systems and singular zeros of polynomial systems	程进三	第九届全国计算机数学学术会议	湘潭	2017.10
8.	素数判定与整数分解	邓映蒲	2017 格密码与数论国际研讨会	长沙	2017.11
9.	The computation of the Galois groups of linear difference equations	冯如勇	微分 Galois 理论以及微分代数群国际研讨会	加拿大	2017.7
10.	Difference Galois groups under specialization	冯如勇	第八届微分代数以及相关问题国际研讨会	奥地利	2017.9
11.	Further results on Butterfly structures with the best known nonlinearity	冯秀涛	中国密码青年论坛	郑州	2017.6

12.	Criteria for Finite Difference Groebner Bases of Normal Binomial Difference Ideals	高小山	ISSAC 2017	德国	2017.7
13.	Sparse Polynomial Interpolation with Finitely Many Values for the Coefficients	高小山	Computer Algebra in Scientific Computing(CASC2017)	北京	2017. 9
14.	Quantum Algorithm for Solving Boolean Equations and Cryptanalysis	高小山	International Workshop on Quantum Computing and Cryptanalysis	北京	2017. 11
15.	Mathematical Aspects of Computer and Information Sciences	高小山	Sparse Rational Function Interpolation with Finitely Many Values for the Coefficients	奥地利	
16.	A glimpse on representation theory of algebras	韩 阳	代数及其应用	中国科学技术大学	2017.5
17.	Singularity Computation of Rational Curves and Surfaces Using Mu-Bases	贾晓红	SIAM conference on Algebraic Geometry	美国	2017.7
18.	How Algebra is Used in Collision Detection	贾晓红	第十届全国几何设计与计算学术会议	烟台	2017.8
19.	有限时间收敛的 gossip 算法存在的充分必要条件	李 博	第一届中国系统科学大会(CSSC2017)	北京	2017.5
20.	Graphical Reduction of Probabilistic Boolean Networks	李 博	第三十六届中国控制会议(CCC2017)	大连	2017.7

21.	Consensus over Quantum Networks: Towards Distributed Quantum Control and Computation	李　博	量子计算与密码分析国际研讨会 (QCCA2017)	北京	2017.11
22.	Automated Geometric Reasoning with Geometric Algebra: Theory and Practice	李洪波	ISSAC 2017	德国	2017.7
23.	Automated Geometric Reasoning and Algebraic Management of Geometric Knowledge	李洪波	Harmonic Analysis and Application	北京	2017.10
24.	Differential Chow Forms and Differential Chow Varieties: an Overview	李　伟	第八届微分代数以及相关问题国际研讨会	奥地利	2017.9
25.	Differential Chow Forms and Differential Chow Varieties: an Overview	李　伟	2017 年中国数学会年会	湘潭	2017.10
26.	Additive Decomposition in Elementary Extensions	李子明	SIAM conference on Algebraic Geometry	美国	2017.7
27.	增强风险与效益意识	刘卓军	恒丰银行干部培训会	昆山	2017.8
28.	大数据的价值追求	刘卓军	鄂尔多斯创新创业论坛	鄂尔多斯	2017.8
29.		潘彦斌	2017 年编码理论与密码学及相关课题国际研讨会	淄博	2017.4
30.	A Broadcast Attack against NTRU	潘彦斌	第五届密码学与云计算安全国际研讨会	运城	2017.6

31.	Computing Hermite Normal Form Faster via Solving System of Linear Equations	潘彦斌	第八届有限域及其应用国际研讨会	北京	2017.11
32.	Broadcast Attacks against NTRU	潘彦斌	International Workshop on Quantum Computing and Quantum Information Processing 2017	北京	2017.11
33.	A New Algorithm for General Factorizations of Multivariate Polynomial Matrices	王定康	ISSAC 2017	德国	2017.7
34.	参数 Groebner 基与几何定理的自动发现	王定康	数学及其交叉学科国际研讨会 2017	武汉	2017.10
35.	PT-对称的非线性波系统	闫振亚	2017 第七届非线性数学物理国际会议暨全国第十四届孤立子与可积系统学术研讨会	北京	2017.8
36.	Nonlinear Waves in Mathematical Physics	闫振亚	2017 上海理工大学可积系统最新进展学术研讨会	上海	2017.11
37.	Nonlinear Waves in integrable systems and nearly integrable systems	闫振亚	第 9 届河姆渡可积系统论坛	宁波	2017.11
38.	Decompositions and ranks of Hankel tensors	叶　科	Householder Symposium XX on Numerical Linear Algebra	美国	2017.6
39.	Tensor network ranks	叶　科	SIAM Conference on Applied Algebraic Geometry	美国	2017.7
40.	Optimization on flag manifolds	叶　科	SIAM Annual Meeting	美国	2017.7

41.	Dimension of tensor networks	叶　科	2017 Meeting of the International Linear Algebra Society	美国	2017.7
42.	Algebraic and geometric aspects of tensors	叶　科	International Conference on Matrix Theory and Application	韩国	2017.12
43.	Binomial partial difference ideals	袁春明	第九届全国计算机数学学术会议	湘潭	2017.10
44.	Private Multi-File Retrieval From Distributed Databases	张志芳	The International Conference on Coding Theory, Cryptography and Related Topics	淄博	2017.4
45.	Computing Multiple Zeros of Polynomial Systems:	支丽红	Foundations of Computational Mathematics	西班牙	2017.7
46.	Irreducible Decomposition of Real Algebraic Sets	支丽红	SIAM Conference on Applied Algebraic Geometry	美国	2017.7
47.	Polynomial Time Interactive Proofs forLinear Algebra with Exponential Matrix Dimensionsand Scalars Given by Polynomial Time Circuits	支丽红	The International Symposium on Symbolic and Algebraic Computation	德国	2017.7
48.	Computing Simple Multiple Zeros of Polynomial SystemsCase of Breath One	支丽红	Computer Algebra in Scientific Computing(CASC2017)	北京	2017. 9

3. 开放课题一览表

序号	课题名称	负责人	职称	工作单位	参加人员	课题开始时间	课题结束时间	总经费（万元）
1	符号计算程序验证	杨争峰	副高级	华东师范大学	支丽红，沈敏捷	2017-2-10	2017-3-5	0.72

2	生物学原理的优化算法	谢福鼎	正高级	辽宁师范大学	王定康	2017-11-6	2017-12-5	1.9
3	Geometric Interpretation to Generative Learning Model	顾险峰	正高级	纽约州立大学石溪分校	贾晓红	2017-10-19	2017-10-28	1
4	非局域可积系统	朱佐农	正高级	上海交通大学	闫振亚	2017-11-6	2017-11-13	0.6
5	可积系统的 Darboux 变换及其应用	周子翔	正高级	复旦大学	闫振亚	2017-11-1	2017-11-8	0.6
6	数控加工中的小线段过渡方法与优化	张立先	中级	武汉工程大学	袁春明	2017-11-7	2017-11-17	0.8
合计	\	\	\	\	\	\	\	5.62

负责人：应为实验室以外人员。
职称：正高级、副高级、中级、初级、其他。
参加人员：除负责人外的其他参与人员。
课题开始时间/课题结束时间：填写格式为“-年-月-日”
总经费：数字。

4. 30 万元以上仪器设备使用情况

序号	设备类型	设备型号	设备名称	设备状况	价格(万元)	实验室研究总机时(小时)	对外服务总机时(小时)	购置时间	性能指标	用途	是否开放
1	购置	XH714-5X	AC 摇篮式五轴联动加工中心	良	75	80	0	2013-03-20	行程 :X Y Z 560 毫米, 410 毫米, 450 毫米；定位精度/重复定位精度 X Y Z, 0.012 / 0.008 毫米；最大快移速度与进给：20 米/分；最大加速度：3 米/秒等	高档数控机床算法研究及实验	否

设备类型：自制、购置、改装；
设备状况：优、良、差；
价格：以万元（人民币）为单位填写，用美元购买的设备按照购买时汇率换算，只能是数字；
实验室研究总机时：研究总机时只需要填写本年度的数据，机时中应包括机器预备、测试、后处理的总机时，只能是数字；
对外服务总机时：服务总机时只需要填写本年度的数据，非本室人员研究工作总机时，只能是数字；
购置时间：填写格式为“-年-月-日”
性能指标：不超过 100 字；
用途：不超过 100 字；
是否开放：非本室人员是否有权使用该仪器，是、否。

第七部分 学委会会议情况

1. 学术委员会名单

序号	姓名	性别	出生年份	职称	学委会职务	工作单位	备注
1.	李邦河	男	1942.07	正高级	主任	中科院数学院	院士
2.	高小山	男	1963-10	正高级	副主任	中科院数学院	
3.	万哲先	男	1927-11	正高级	委员	中科院数学院	院士
4.	陆汝钤	男	1935-02	正高级	委员	中科院数学院	院士
5.	张景中	男	1936-12	正高级	委员	中科院成都计算机研究所	院士
6.	林惠民	男	1947-11	正高级	委员	中科院软件所	院士
7.	黄民强	男	1960-10	正高级	委员	中科院系统所	院士
8.	王东明	男	1961-07	正高级	委员	北京航空航天大学/广西民族大学	欧洲科学院院士
9.	陈永川	男	1964-03	正高级	委员	南开大学	院士
10.	王小云	女	1966-08	正高级	委员	清华大学	院士
11.	张继平	男	1958-07	正高级	委员	北京大学	
12.	宗传明	男	1962-09	正高级	委员	天津大学	
13.	林东岱	男	1964-04	正高级	委员	中科院信息工程研究所	
14.	陈发来	男	1966-11	正高级	委员	中国科学技术大学	
15.	李洪波	男	1968-03	正高级	委员	中科院数学院	

学委会职务：主任、副主任、委员、顾问
备注：如是院士，可在备注中标注。

2. 学术委员会会议

会议年度	2017 年
会议时间	2017.3.30
地点	中国科学院数学与系统科学研究院南楼 420 会议室
学委会委员出席人员名单	李邦河,高小山,万哲先,陆汝钤,林惠民,张继平,王东明,宗传明,林东岱,王小云,李洪波
学委会委员缺席人员名单	张景中,黄民强,陈永川,陈发来
会议纪要	中国科学院数学机械化重点实验室第四届学术委员会第三次会议于 2017 年 3 月 30 日在中国科学院数学与系统科学研究院南楼 420 召开。实验室学术委员会主任李邦河院士，副主任高小山研究员，万哲先院士，陆汝钤院士，林惠民院士，北京大学张继平教授，北京航空航天大学/广西民族大学王东明教授，北京大学宗传明教授，中科院信息工

	程研究所林东岱研究员，清华大学王小云教授，实验室主任李洪波研究员等 11 位学术委员会委员参加了本次会议。中国科学院前沿科学与教育局重点实验室处白雪瑞副处长也应邀参加了本次会议。此外实验室副主任邓映蒲研究员，支丽红研究员，数学院科研处主管实验室事宜的王晓欢博士也参加了本次会议。 会议由实验室学术委员会主任李邦河院士主持。首先实验室主任李洪波研究员从成果进展、学术活动、实验室建设等方面汇报了实验室 2016 年的各项工作。随后，冯如勇副研究员、潘彦斌副研究员分别作了“线性差分方程 Galois 理论中的正问题”和“对 Hanser-Slamanig 等价类上保结构签名体制的安全性分析”的学术报告。 随后,学术委员会对实验室 2016 年的组织工作与科研成果予以了充分肯定，对实验室现状及未来发展方向进行了深入讨论。期间，实验室主任李洪波研究员对实验室即将开辟的量子计算研究方向进行了总体介绍与展望；高小山研究员具体介绍了实验室即将承担的科技委批准的量子算法项目，该项目将实验室长期积累的数学机械化算法和密码分析的研究经验与量子相关前沿课题相结合，重点研究量子算法。该项目是实验室继科技部 973 项目、基金委群体项目之后承担的又一重大项目，将为实验室未来的科研工作提供充裕的经费支持；林惠民院士进一步分析了量子计算的研究前景，认为目前虽然量子算法的可研究空间很大，但寻找量子算法模型及界定何种算法适用于发展量子算法还很困难。王小云教授也表达了同样的观点，作为该项目的参与者，王教授认为应从已取得进展的密码分析算法入手，结合某具体问题，逐步积累在量子算法方面的经验。陆汝钤院士也指出，目前量子算法很少，但目前已有科学家将量子算法的思想运用到人工智能研究中。结合实验室的研究特点，可尝试将符号推理与符号计算的思想运用到量子计算中。 学术委员会委员同时对实验室的发展提出了意见和建议。王东明教授指出，实验室奠基人吴先生研究数学机械化理论已经 40 余年，推动了整个学科的发展，现在活跃在科研一线的年轻人应该承担起学科发展的重任，思考如何在国内外同行中争得上游，与专家前辈和兄弟院校协力在吴先生的工作基础上开辟拓展新方向。林东岱研究员充分赞赏了潘彦斌副研究员的工作，鼓励其在已有成果基础上继续寻求突破。目前，数学机械化方向迫切需要新的突破口与里程碑，才能赢得国内外同行的广泛认可。宗传明教授认为应重视实际问题的研究，而实验室一直以来的数控技术的研究就是将实际问题转换为数学问题并最终

	用数学解决实际问题的良好典范。张继平教授对实验室的发展谈了两点看法：一：吴先生的数学机械化理论是不可多得的有世界影响力的成果，目前数学机械化的学科发展及队伍扩大都很不容易，作为上级单位，科学院应该建立保护数学机械化发展的具体措施，使数学机械化的研究逐代传承下去。他赞扬了实验室的代表性研究成果。二：尽管目前数学学科对应用、算法方面关注度较高，但理论研究的根不能丢。林惠民院士也认为数学院在国际上享有盛誉，科学院应对数学院、对数学机械化中心给予更多扶持。虽然目前实验室开辟了量子算法的新研究领域，但对吴方法等经典算法的研究不能丢弃。王小云教授建议实验室以能否改进吴方法作为挑选学生的依据，鼓励吸引更多力量研究发展吴方法。陆汝钤院士建议实验室将数学机械化的算法软件开源，让更多人使用，从而推动数学机械化的发展。最后，李邦河院士对各位委员提出的宝贵意见和建议表示了感谢，同时建议实验室将吴方法和 Groebner 基进行详尽的比对,让大家充分了解吴方法和 Groebner 基的优缺点。实验室也应对研究吴方法的老师给予特别支持,鼓励科研人员多写论文，使吴方法引起更广泛的关注，使数学机械化学科充分发扬光大。

学委会委员出席人员名单：依次列出学委会委员出席学委会会议人员名单，姓名之间请用,（英文半角逗号）分隔；

学委会委员缺席人员名单：依次列出学委会委员缺席学委会会议人员名单，姓名之间请用,（英文半角逗号）分隔；

第八部分 审核意见

（实验室承诺所填内容属实，数据准确可靠）

本人代表实验室承诺年报中所有信息真实可靠，若有失实和造假行为，本人愿承担一切责任。

实验室主任：

年 月 日

依托单位对实验室的年度考核意见：

依托单位负责人签字：

（单位公章）

年 月 日