批准立项年份	2006.8.29
通过验收年份	2007.5.13

教育部重点实验室年度报告

（ 2016 年 1 月 —— 2016 年 12 月 ）

实验室名称：密码技术与信息安全教育部重点实验室

实验室主任：王小云

实验室联系人/联系电话：王美琴/0531-88363280

E-mail 地址：mqwang@sdu.edu.cn

依托单位名称：山东大学

依托单位联系人/联系电话：盛楠/0531-88369279

2017 年 3 月 29 日 填报

填写说明

一、年度报告中各项指标只统计当年产生的数据，起止时间为 1 月 1 日至 12 月 31 日。年度报告的表格行数可据实调整，不设附件，请做好相关成果支撑材料的存档工作。年度报告经依托高校考核通过后，于次年 3 月 31 日前在实验室网站公开。

二、**“研究水平与贡献”**栏中，各项统计数据均为本年度由实验室人员在本实验室完成的重大科研成果，以及通过国内外合作研究取得的重要成果。其中：

1. **“论文与专著”**栏中，成果署名须有实验室。专著指正式出版的学术著作，不包括译著、论文集等。未正式发表的论文、专著不得统计。

2. **“奖励”**栏中，取奖项排名最靠前的实验室人员，按照其排名计算系数。系数计算方式为：1/实验室最靠前人员排名。例如：在某奖项的获奖人员中，排名最靠前的实验室人员为第一完成人，则系数为 1；若排名最靠前的为第二完成人，则系数为 1/2=0.5。实验室在年度内获某项奖励多次的，系数累加计算。部委（省）级奖指部委（省）级对应国家科学技术奖相应系列奖。一个成果若获两级奖励，填报最高级者。未正式批准的奖励不统计。

3. **“承担任务研究经费”**指本年度内实验室实际到账的研究经费、运行补助费和设备更新费。

4. **“发明专利与成果转化”**栏中，某些行业批准的具有知识产权意义的国家级证书（如：新医药、新农药、新软件证书等）视同发明专利填报。国内外同内容专利不得重复统计。

5. **“标准与规范”**指参与制定国家标准、行业/地方标准的数量。

三、**“研究队伍建设”**栏中：

1. 除特别说明统计年度数据外，均统计相关类型人员总数。固定人员指高等学校聘用的聘期 2 年以上的全职人员；流动人员指访问学者、博士后研究人员等。

2. **“40 岁以下”**是指截至当年年底，不超过 40 周岁。

3. **“科技人才”**和**“国际学术机构任职”**栏，只统计固定人员。

4. **“国际学术机构任职”**指在国际学术组织和学术刊物任职情况。

四、**“开放与运行管理”**栏中：

1. **“承办学术会议”**包括国际学术会议和国内学术会议。其中，国内学术会议是指由主管部门或全国性一级学会批准的学术会议。

2. **“国际合作项目”**包括实验室承担的自然科学基金委、科技部、外专局等部门主管的国际科技合作项目，参与的国际重大科技合作计划/工程（如：ITER、CERN 等）项目研究，以及双方单位之间正式签订协议书的国际合作项目。

一、简表

<table>
<tr><td colspan="2">实验室名称</td><td colspan="6">密码技术与信息安全教育部重点实验室</td></tr>
<tr><td colspan="2" rowspan="4">研究方向
(据实增删)</td><td>研究方向 1</td><td colspan="5">密码理论</td></tr>
<tr><td>研究方向 2</td><td colspan="5">数论代数安全计算</td></tr>
<tr><td>研究方向 3</td><td colspan="5">密码技术与应用</td></tr>
<tr><td>研究方向 4</td><td colspan="5">网络与系统安全</td></tr>
<tr><td rowspan="2">实验室主任</td><td>姓名</td><td>王小云</td><td>研究方向</td><td colspan="3">信息安全</td></tr>
<tr><td>出生日期</td><td>1966.08</td><td>职称</td><td>教授</td><td>任职时间</td><td>2007</td></tr>
<tr><td rowspan="4">实验室副主任
(据实增删)</td><td>姓名</td><td>王美琴</td><td>研究方向</td><td colspan="3">密码理论、密码技术与应用、网络与系统安全</td></tr>
<tr><td>出生日期</td><td>1974.07</td><td>职称</td><td>教授</td><td>任职时间</td><td>2013</td></tr>
<tr><td>姓名</td><td>王明强</td><td>研究方向</td><td colspan="3">密码理论、数论代数安全计算、密码技术与应用</td></tr>
<tr><td>出生日期</td><td>1970.09</td><td>职称</td><td>教授</td><td>任职时间</td><td>2015</td></tr>
<tr><td rowspan="2">学术委员会主任</td><td>姓名</td><td>蔡吉人</td><td>研究方向</td><td colspan="3">信息安全</td></tr>
<tr><td>出生日期</td><td>1935.07</td><td>职称</td><td>院士</td><td>任职时间</td><td>2007</td></tr>
<tr><td rowspan="10">研究水平与贡献</td><td rowspan="2">论文与专著</td><td>发表论文</td><td>SCI</td><td>12 篇</td><td>EI</td><td>16 篇</td></tr>
<tr><td>科技专著</td><td>国内出版</td><td>部</td><td>国外出版</td><td>部</td></tr>
<tr><td rowspan="4">奖励</td><td>国家自然科学奖</td><td>一等奖</td><td>项</td><td>二等奖</td><td>项</td></tr>
<tr><td>国家技术发明奖</td><td>一等奖</td><td>项</td><td>二等奖</td><td>项</td></tr>
<tr><td>国家科学技术进步奖</td><td>一等奖</td><td>项</td><td>二等奖</td><td>项</td></tr>
<tr><td>省、部级科技奖励</td><td>一等奖</td><td>项</td><td>二等奖</td><td>项</td></tr>
<tr><td>项目到账总经费</td><td>443 万元</td><td>纵向经费</td><td>409 万元</td><td>横向经费</td><td>34 万元</td></tr>
<tr><td rowspan="2">发明专利与成果转化</td><td>发明专利</td><td>申请数</td><td>4 项</td><td>授权数</td><td>1 项</td></tr>
<tr><td>成果转化</td><td>转化数</td><td>项</td><td>转化总经费</td><td>万元</td></tr>
<tr><td>标准与规范</td><td>国家标准</td><td colspan="2">1 项</td><td>行业/地方标准</td><td>项</td></tr>
</table>

<table>
<tr><td rowspan="8">研究队伍建设</td><td rowspan="6">科技人才</td><td colspan="2">实验室固定人员</td><td>35 人</td><td colspan="2">实验室流动人员</td><td>1 人</td></tr>
<tr><td colspan="2">院士</td><td>人</td><td colspan="2">千人计划</td><td>长期 人
短期 人</td></tr>
<tr><td colspan="2">长江学者</td><td>特聘 2 人
讲座 人</td><td colspan="2">国家杰出青年基金</td><td>2 人</td></tr>
<tr><td colspan="2">青年长江</td><td>人</td><td colspan="2">国家优秀青年基金</td><td>人</td></tr>
<tr><td colspan="2">青年千人计划</td><td>人</td><td colspan="2">其他国家、省部级
人才计划</td><td>人</td></tr>
<tr><td colspan="2">自然科学基金委创新群体</td><td>个</td><td colspan="2">科技部重点领域创新团队</td><td>个</td></tr>
<tr><td rowspan="3">国际学术机构任职
(据实增删)</td><td colspan="2">姓名</td><td colspan="3">任职机构或组织</td><td>职务</td></tr>
<tr><td colspan="2">刘建亚</td><td colspan="3">Advances in Mathematics of Communications</td><td>联合主编</td></tr>
<tr><td colspan="2">王小云</td><td colspan="3">Journal of Cryptology</td><td>编委</td></tr>
<tr><td>访问学者</td><td colspan="2">国内</td><td>0 人</td><td colspan="2">国外</td><td>0 人</td></tr>
<tr><td>博士后</td><td colspan="2">本年度进站博士后</td><td>1 人</td><td colspan="2">本年度出站博士后</td><td>0 人</td></tr>
<tr><td rowspan="4">学科发展与人才培养</td><td>依托学科
(据实增删)</td><td>学科 1</td><td>数学</td><td>学科 2</td><td>计算机</td><td>学科 3</td><td>网络空间安全</td></tr>
<tr><td>研究生培养</td><td colspan="2">在读博士生</td><td>31 人</td><td colspan="2">在读硕士生</td><td>151 人</td></tr>
<tr><td>承担本科课程</td><td colspan="3">2266 学时</td><td colspan="2">承担研究生课程</td><td>1317 学时</td></tr>
<tr><td>大专院校教材</td><td colspan="3">部</td><td colspan="2"></td><td></td></tr>
<tr><td rowspan="4">开放与运行管理</td><td>承办学术会议</td><td>国际</td><td colspan="2">1 次</td><td>国内
(含港澳台)</td><td colspan="2">次</td></tr>
<tr><td colspan="4">年度新增国际合作项目</td><td colspan="3">项</td></tr>
<tr><td colspan="2">实验室面积</td><td colspan="2">6657 M^2</td><td>实验室网址</td><td colspan="2">www.infosec.sdu.edu.cn</td></tr>
<tr><td colspan="2">主管部门年度经费投入</td><td colspan="2">(直属高校不填)万元</td><td colspan="2">依托单位年度经费投入</td><td>20 万元</td></tr>
</table>

二、研究水平与贡献

1、主要研究成果与贡献

结合研究方向，简要概述本年度实验室取得的重要研究成果与进展，包括论文和专著、标准和规范、发明专利、仪器研发方法创新、政策咨询、基础性工作等。总结实验室对国家战略需求、地方经济社会发展、行业产业科技创新的贡献，以及产生的社会影响和效益。

2016 年实验室立足基础理论研究，面向国家战略需求与地方经济发展，取得一系列重要研究成果与进展。

王小云教授带领其研究团队在密码分析领域提出了两类重要的新型攻击方法：1. 统计积分攻击新方法. 积分攻击已成为分组密码算法的通用攻击方法，基于概率为一的平衡特性作为区分器，为了使得积分区分器的覆盖轮数增长，攻击者不得不遍历更多的明文比特以使得平衡特性依然成立。然而这限制了积分攻击在一些算法分析中的应用。团队与 ISO 标准密码算法 PRESENT 设计者 Andrey Bogdanov 等合作，基于超几何分布和多项分布构造不同的概率分布构建统计模型，从而构建了统计积分攻击的新方法。新方法解决了必须遍历部分明文比特的难题，为密码学领域积分攻击方法增添了新的技术，成功破解 SKIPJACK 变种算法，SKIPJACK 算法是美国国家安全局设计的首个分组密码算法。该结果发表于 FSE 2016。2. 基于 MILP 的 ARX 类算法的差分自动化搜索新方法。近年来，混合整数线性规划(MILP)已经被成功用于搜索分组密码算法的差分特征和线性近似，而且也在一些算法中取得了重要结果。然而，MILP 自动搜索算法尚不能用于搜索 ARX 类算法的差分和线性路线。团队提出了 ARX 密码算法差分和线性路线的 MILP 自动搜索算法，为国际密码学界 ARX 类算法的安全性评估提供了有效而便捷的工具。将我们的工具应用于美国国家安全局设计的分组密码算法 SPECK 的攻击中，比著名密码学家 Alex Biryukov 教授给出的攻击提升了 5 轮（大分组），这种提升在密码分析领域是突破性的。进一步证明了该方法的有效性。该结果发表于 FSE 2016。

在网络与系统安全方向，李庆忠和崔立真教授带领的研究团队针对区块链底层基础支撑软件关键技术进行研究，对分布式账本、共识协议、许可节点准入、

快速检索和数据隐私保护等区块链基础软件核心技术进行研究，并重点开展自主可控的许可区块链支撑平台基础核心软件开发，建立面向公共服务、政务服务等领域、多中心的、可扩展的的许可区块链支撑平台。通过提供支持二次开发的区块链平台 API，实现数字证照、数字凭据等的快速开发，解决了公共服务、政务服务等领域信息可信传递的难题，可以实现信任建立和信任传递，促进信用社会的建立。

2016 年度，刘建亚教授与吴杰、赵永强合作，证明了 Manin 猜想对于一种特殊情形的丢番图方程成立，并给出了相应的解的个数的渐进公式。此外，以刘建亚教授为带头人的“数论”创新团队被列为教育部 72 个建设成效显著的团队，并给予滚动支持。

同时，实验室积极推动密码算法标准化进程，推动制定国家标准一项。（王小云，于红波，信息安全技术 SM3 密码杂凑算法，GB/T 32905-2016，全国信息安全标准化技术委员会，2016.08.09。）

2、承担科研任务

概述实验室本年度科研任务总体情况。

2016 年共承担 “973”计划、国家自然科学基金、教育部、科技部各类科研项目 39 项，总经费 2279 万元，2016 年到账经费 443 万元。其中：

来自科技部的项目 6 项，总经费共 635 万元，到账经费 214 万元。

来自国家自然科学基金委项目 10 项，经费共 664 万元，到账经费 84 万元。

来自教育部的项目 2 项，总经费 350 万元，到账经费 25 万元。

来自山东省科技厅的项目 12 项，总经费 452 万元，到账经费 50 万元。

横向课题 3 项，总经费 55 万元，到账经费 34 万元。

请选择本年度内主要重点任务填写以下信息:

序号	项目/课题名称	编号	负责人	起止时间	经费(万元)	类别
1	相关数学问题研究在密码分析和设计中的应用*	2013CB834205	王美琴	2013.01-2017.08	100	973 子课题
2	相关数学问题研究在密码分析和设计中的应用*	2013CB834205	王明强	2013.01-2017.12	95	973 子课题
3	数论	IRT-16R43	刘建亚	2017.01-2019.12	300	教育部创新团队
	自守表示与代数簇的算术问题	11531008	刘建亚	2016.01-2020.12	230	重点项目
4	新世纪优秀人才支持计划	NECT-13-0350	王美琴	2014.01-2016.12	50	新世纪计划
5	新型密码算法及其安全性分析*	61133013	王美琴	2012.01-2016.12	50	重点项目子课题
6	椭圆曲线上与密码算法相关的计算问题	61272035	王明强	2012.01-2016.12	61	面上项目
7	分组密码算法的新型分析与设计理论的研究	61572293	王美琴	2016.01-2019.12	76	面上项目
8	多项式代数及自由结合代数的自同构和导子	11371165	张顺华	2014.01-2017.12	10	面上项目
9	面向复杂大数据应用的数据动态协同分布与均衡控制关键技术研究	61572295	崔立真	2015.08-2019.12	77.2	面上项目
10	云计算环境下面向多租户应用的数据隐私保护机制研究	61272241	史玉良	2013.01-2016.12	80	面上项目
11	863**********	*******	王美琴	2015.07-2016.06	60	863 计划
12	面向大数据创新研发的支撑环境关键技术研究与应用示范	SQ2015IMC600006	崔立真	2015.10-2017.10	259	科技部创新方法工作专项
13	超大规模关系型数据管理关键技术及系统*	2016YFB1000602	李庆忠	2016.07-2019.06	32	国家重点研发计划项目
14	无界互联电子商务关键技术研发与应用示范	2015GGX101015	崔立真	2015.06-2016.12	25	山东省重点研发计划
15	支持即时分析的大数据平台研发	2015GGX101007	李庆忠	2015.06-2016.12	25	山东省重点研发计划

16	支持应用敏捷自适应与互动创新的高可信大数据应用支撑平台关键技术研发	2016ZDJS01A09	史玉良	2016.01-2018.12	100	山东省重点研发计划（重大关键技术）
17	云计算大数据分析 PaaS 平台研发与应用示范	2015ZDJQ01002	史玉良	2015.9-2017.12	30	山东省科技重大专项
18	高并发移动互联关键技术研发及示范	2015ZDXX0201B03	崔立真	2015.9-2017.12	100	山东省科技重大专项
19	运输多元数据智能分析及决策技术的研发及示范	2015ZDXX0201A04	史玉良	2015.9-2017.12	60	山东省科技重大专项

注：请依次以国家重大科技专项、“973”计划（973）、“863”计划（863）、国家自然科学基金（面上、重点和重大、创新研究群体计划、杰出青年基金、重大科研计划）、国家科技（攻关）、国防重大、国际合作、省部重大科技计划、重大横向合作等为序填写，并在类别栏中注明。只统计项目/课题负责人是实验室人员的任务信息。只填写所牵头负责的项目或课题。**若该项目或课题为某项目的子课题或子任务，请在名称后加*号标注。**

三、研究队伍建设

1、各研究方向及研究队伍

研究方向	学术带头人	主要骨干
1．密码理论	王小云	王明强
2．数论代数安全计算	刘建亚	吕广世
3．密码技术与应用	王美琴	孔凡玉
4．网络与系统安全	李庆忠	崔立真

2.本年度固定人员情况

序号	姓名	类型	性别	学位	职称	年龄	在实验室工作年限
1	张顺华	研究人员	男	博士	教授	54	2006 至今
2	周大水	研究人员	男	硕士	教授	54	2006 至今
3	任秀敏	研究人员	女	博士	教授	53	2008 至今
4	刘建亚	研究人员	男	博士	教授	52	2006 至今
5	李庆忠	研究人员	男	博士	教授	51	2008 至今
6	郑永清	研究人员	男	博士	研究员	51	2008 至今
7	王小云	研究人员	女	博士	教授	50	2006 至今
8	王新军	研究人员	男	博士	教授	48	2008 至今
9	张世栋	研究人员	男	博士	教授	47	2008 至今
10	王明强	研究人员	男	博士	教授	46	2006 至今
11	王美琴	研究人员	女	博士	教授	42	2006 至今
12	吕广世	研究人员	男	博士	教授	41	2006 至今
13	崔立真	研究人员	男	博士	教授	40	2008 至今
14	肖宗水	研究人员	男	博士	副教授	54	2006 至今
15	孙秋梅	研究人员	女	硕士	副教授	51	2006 至今
16	张岳公	研究人员	男	博士	副教授	49	2006 至今
17	董国庆	研究人员	男	硕士	副教授	49	2008 至今
18	李　晖	研究人员	女	博士	副教授	49	2008 至今
19	任国珍	研究人员	男	硕士	副教授	46	2008 至今
20	王　华	研究人员	男	博士	副教授	46	2006 至今
21	陈志勇	研究人员	男	博士	副教授	46	2013 至今
22	孙　明	研究人员	男	硕士	副教授	44	2008 至今
23	郭山清	研究人员	男	博士	副教授	40	2015 至今

24	孔凡玉	研究人员	男	博士	副教授	38	2006 至今
25	刘 磊	研究人员	男	博士	副教授	36	2015 至今
26	史玉良	研究人员	男	博士	副教授	38	2008 至今
27	孔兰菊	研究人员	女	博士	副教授	38	2012 至今
28	王光辉	研究人员	男	博士	副教授	37	2015 至今
29	纪广华	研究人员	男	博士	副教授	36	2010 至今
30	魏普文	研究人员	男	博士	副教授	35	2010 至今
31	徐 进	管理人员	男	博士	实验师	36	2008 至今
32	刘晓东	研究人员	男	博士	讲师	41	2006 至今
33	张国艳	研究人员	女	博士	讲师	39	2008 至今
34	闫中敏	研究人员	女	博士	讲师	39	2008 至今
35	王 薇	研究人员	女	博士	讲师	33	2009 至今

注：（1）固定人员包括研究人员、技术人员、管理人员三种类型，应为所在高等学校聘用的聘期 2 年以上的全职人员。（2）“在实验室工作年限”栏中填写实验室工作的聘期。

3、本年度流动人员情况

序号	姓名	类型	性别	年龄	职称	国别	工作单位	在实验室工作期限
1	葛爱军	博士后	32	男	讲师	中国	信息工程大学	2017.01-2019.01
2								
3								
4								
5								

注：（1）流动人员包括“博士后研究人员、访问学者、其他”三种类型，请按照以上三种类型进行人员排序。（2）在“实验室工作期限”在实验室工作的协议起止时间。

四、学科发展与人才培养

1、学科发展

简述实验室所依托学科的年度发展情况，包括科学研究对学科建设的支撑作用，以及推动学科交叉与新兴学科建设的情况。

实验室依托于数学学科和计算机学科两个学科。山东大学数学学院拥有基础数学、计算数学、运筹学与控制论、应用数学、概率论与数理统计五个二级重点学科，以及系统理论、信息安全、金融数学与金融工程等共计 8 个博士点，并设有数学和系统科学两个博士后流动站；概率论与金融数学、数论与信息安全的研究位列世界前列，形成了重要的国际影响。数学学院下设数学和应用数学、信息与计算科学、统计学、信息安全四个系，设基础数学、科学计算与软件、应用数学、系统与运筹学、控制与系统科学、概率论与数理统计、信息安全七个研究所。并设有密码技术与信息安全教育部重点实验室，风险分析与随机计算山东省重点实验室，金融数学基地为山东省高级金融人才培养基地。拥有一支敬业博学的师资队伍，其中教授 51 名，副教授 44 名，博士生导师 38 名，硕士生导师 60 余名。现有中国科学院院士 1 名、教育部“长江学者奖励计划”特聘教授 4 名，“国家杰出青年基金”获得者 4 名，中组部“千人计划”国家特聘教授 2 名，国家高等学校教学名师 2 名，“泰山学者”4 名。

山东大学计算机科学与技术学院拥有计算机科学与技术和软件工程两个一级学科博士学位授权点，计算机软件与理论、计算机应用技术、计算机系统结构、数字媒体技术和艺术四个博士学位授权点和电子商务与信息技术硕士点，并设有计算机科学与技术和软件工程博士后流动站。形成了人机交互与虚拟现实、软件与数据工程、智能信息处理、智能计算、大数据管理与分析、机器学习与媒体分析、信息安全与密码学、体系结构与高性能计算、计算机网络等多个研究方向。设有人机交互与虚拟现实、软件与数据工程、智能信息处理三个研究中心和软件、网络与信息安全、体系结构与高性能计算三个研究所，计算机科学与技术、电子商务两个教学系以及计算机基础技术教学部、计算中心等单位。并设有电子商务交易技术国家工程实验室、教育部密码技术与信息安全重点实验室、教育部数字媒体技术工程研究中心、山东省软件工程重点实验室、山东省电子政务信息安全

实验室、山东省制造业信息化工程技术研究中心、山东省 CIMS 工程技术研究中心、山东省应用软件工程技术研究中心、山东省高性能计算中心等科研机构，是山东省计算机及软件人才的重要培养基地。学院现有教职工 160 人，专任教师 111 人，其中博士生导师 21 人，教授 33 人、副教授 57 人。

2、科教融合推动教学发展

简要介绍实验室人员承担依托单位教学任务情况，主要包括开设主讲课程、编写教材、教改项目、教学成果等，以及将本领域前沿研究情况、实验室科研成果转化为教学资源的情况。

实验室成员结合专业领域最新研究进展，不断丰富教学内容，调动学生参与科研的积极性，注重培养学生的创新精神和能力。2016 年度承担信息安全专业、数论专业、计算机专业本科与研究生的教学工作如下：

1. 本科课程：应用密码学、计算机网络基础、网络安全、数字签名与认证、数论基础、数据库系统、软件服务工程、面向对象技术等合计 2266 课时；
2. 研究生课程包括：算法数论与密码学（博士）、对称密码的分析与设计（博士）、密码算法的分析与设计、对称密码、算法数论、椭圆曲线基础、网络攻击与防御、密码实现技术、自守形式、代数数论、数据分析技术、大规模数据管理等合计 1317 课时。

3、人才培养

（1）人才培养总体情况

简述实验室人才培养的代表性举措和效果，包括跨学科、跨院系的人才交流和培养，与国内、国际科研机构或企业联合培养创新人才等。

2016 年，实验室主任王小云获得全国优秀科技工作者称号（中共中央组织部，人事部，中国科学技术协会）以及网络安全杰出人才奖（中国互联网发展基金会网络安全专项基金办公室）。实验室成员肖宗水获得山东省泰山产业领军人才（山东省政府）以及济南市引进海内外高层次创新人才（5150 人才）（济南市政府）称号；成员史玉良获得济南市引进海内外高层次创新人才（5150 人才）称号（济南市政府）。

2016 年共培养硕士生 26 人，博士生 10 人，为国家密码相关部门输送了一大批优秀人才。2016 年招收来自全国各大院校的优秀博士生 7 人、硕士生 68 人。在研究生培养方面，采取跨学校跨院系的培养模式，实验室通过租用专线的方式开通了清华大学-山东大学的点对点远程视频教学系统，开设了清华-山大的研究生研讨班模式。此外，研究团队中部分博士研究生在修完课程后，将去清华大学继续进行交流学习，充分发挥两校的教师资源，使得研究生能够得到不同学校的培养模式的学习，达到高效交流学习的目的。通过上述措施，进一步增强了学生的学术交流能力，开阔了科研视野。

在国际联合培养方面，实验室派出博士生崔婷婷赴新加坡南洋理工大学进行为期一年的合作研究。推动并选拔优秀学生积极参与国际国内前沿重要会议，如 FSE2016 会议（德国），ChinaCrypt 2016（中国），Inscrypt 2016（中国），促进学生与国内外同行深入交流。同时实验室鼓励学生参加相关竞赛，2016 年 12 月 16 日至 17 日，博士生崔婷婷、硕士生胡凯与硕士生陈师尧，参加了由教育部高等学校数学类专业教学指导委员会举办的“密码数学挑战赛”，获得二等奖。

（2）研究生代表性成果（列举不超过 3 项）

简述研究生在实验室平台的锻炼中，取得的代表性科研成果，包括高水平论文发表、国际学术会议大会发言、挑战杯获奖、国际竞赛获奖等。

(1) 董晓阳，博士，其论文 Chosen-Key Distinguishers on 12-Round Feistel-SP and 11-Round Collision Attacks on Its Hashing Modes 发表在 FSE 2017, IACR Transactions on Symmetric Cryptology，2016.11.10，2016(No.1)：1~32。

(2) 陈怀凤，博士生，其论文 Improved Linear Hull Attack on Round-Reduced Simon with Dynamic Key-guessing Techniques 发表在 FSE 2016 会议（德国，波鸿，2016 年 3 月 20 日-3 月 23 日），并作大会报告。

(3) 付凯，硕士生，其论文 MILP-Based Automatic Search Algorithms for Differential and Linear Trails for Speck 发表在 FSE 2016 会议（德国，波鸿，2016 年 3 月 20 日-3 月 23 日），并作大会报告。

（3）研究生参加国际会议情况（列举 5 项以内）

序号	参加会议形式	学生姓名	硕士/博士	参加会议名称及会议主办方	导师
1	大会发言、口头报告、发表会议论文	陈怀凤	博士	FSE 2016, Ruhr University Bochum	王小云
2	大会发言、口头报告、发表会议论文	付凯	硕士	FSE 2016, Ruhr University Bochum	王美琴
3	大会发言、口头报告、发表会议论文	王绍梅	硕士	Inscrypt 2016, 中国科学院	王美琴
4	大会发言、口头报告	朱冰心	硕士	Inscrypt 2016, 中国科学院	魏普文
5					

注：请依次以参加会议形式为大会发言、口头报告、发表会议论文、其他为序分别填报。**所有研究生的导师必须是实验室固定研究人员。**

五、开放交流与运行管理

1、开放交流

（1）开放课题设置情况

简述实验室在本年度内设置开放课题概况。

为积极促进与国内外专家的合作与交流，实验室设立开放课题，资助与实验室研究方向相关的研究课题。2016 年，共批准来自上海交通大学、北京印刷学院、中国科学技术大学的开放课题申请 3 项，经费额度合计 15 万元。

序号	课题名称	经费额度	承担人	职称	承担人单位	课题起止时间
1	安全高效的新型功能加密体制研究	5	龙宇	讲师	上海交通大学	2016.01 - 2017.12
2	基于格理论可证明安全数字签名算法的研究	5	李子臣	教授	北京印刷学院	2016.01 - 2017.12
3	紧耦合秘密共享研究	5	苗付友	副教授	中国科学技术大学	2016.01 - 2017.12

注：职称一栏，请在职人员填写职称，学生填写博士/硕士。

（2）主办或承办大型学术会议情况

序号	会议名称	主办单位名称	会议主席	召开时间	参加人数	类别
1	第一届众志科学与工程国际会议（ICCSE2016）	电子商务交易技术国家工程实验室	Cyril Leung, Chunyan Miao, Chengqi Zhang	2016.07.27-30	240	全球性

注：请按全球性、地区性、双边性、全国性等类别排序，并在类别栏中注明。

（3）国内外学术交流与合作情况

请列出实验室在本年度内参加国内外学术交流与合作的概况，包括与国外研究机构共建实验室、承担重大国际合作项目或机构建设、参与国际重大科研计划、在国际重要学术会议做特邀报告的情况。请按国内合作与国际合作分类填写。

国际合作：

（1）2016.04.09-2016.04.15，王小云教授赴美国参加国际标准化组织 ISO/IEC SC27 工作组会议；

（2）2016.06.09-2016.06.15，王小云教授赴俄罗斯参加密码学现状研讨会 ；

（3）2016.01.02-2016.01.07，王小云教授、王美琴教授赴德国波鸿参加对称密码研讨会；

（4）2016.03.20-2016.03.23，王美琴教授、博士生陈怀凤、硕士生付凯付德国波鸿参加 FSE 2016；

（5）2016.07，崔立真教授、李庆忠教授、郑永清教授、闫中敏副教授赴加拿大温哥华参加 ICCSE2016。

国内合作交流：

（1） 2016.08.30-09.01，王小云教授、王美琴教授、学生崔婷婷、刘瑜、王绍梅、胡凯、尤瑞英、李艳斌赴银川参加“中国密码学会密码数学理论专委会 2016 年学术研讨会”;

（2） 2016.09.23-24，孔凡玉副教授、魏普文副教授、王薇讲师、学生孙玲、赵艳敏、朱冰心赴杭州参加“中国密码学年会 2016 年会（ChinaCrypt 2016）”;

（3） 2016.11.04 – 11.6，硕士生王绍梅、朱冰心赴北京参加“第 12 届信息安全与密码学学术会议（Inscrypt 2016）”。

（4）科学传播

简述实验室本年度在科学传播方面的举措和效果。

为普及 SM3 密码杂凑算法，加快 SM3 算法在工业界的进一步推广，实验室主任王小云教授受邀撰写文章《SM3 密码杂凑算法》，全面介绍了 SM3 算法知识、当前主流分析技术及推广应用情况，为相关从业人员学习和应用 SM3 算法提供了重要参考。

2、运行管理

（1）学术委员会成员

序号	姓名	性别	职称	年龄	所在单位	是否外籍
1	蔡吉人	男	院士	81	北京信息科学技术研究院	否
2	彭实戈	男	院士	69	山东大学	否
3	展　涛	男	教授	53	教育部教育管理信息中心	否
4	李兆宗	男	研究员	51	北京信息科学技术研究院	否
5	赵　丹	男	高级工程师	52	国家密码管理局商用密码管理办公室	否
6	裴定一	男	教授	75	广州大学	否
7	金晨辉	男	教授	50	信息工程大学	否
8	陈克非	男	教授	57	杭州师范大学	否
9	韩正甫	男	教授	53	中国科技大学	否
10	宗传明	男	教授	54	北京大学	否
11	徐茂智	男	教授	54	北京大学	否
12	林东岱	男	研究员	52	中国科学院信息工程研究所	否
13	刘建伟	男	教授	52	北京航空航天大学	否
14	胡　磊	男	研究员	49	中国科学院信息工程研究所	否
15	刘建亚	男	教授	52	山东大学	否
16	王小云	女	教授	50	山东大学	否

（2）学术委员会工作情况

请简要介绍本年度召开的学术委员会情况，包括召开时间、地点、出席人员、缺席人员，以及会议纪要。

（3）主管部门和依托单位支持情况

简述主管部门和依托单位本年度为实验室提供实验室建设和基本运行经费、相对集中的科研场所和仪器设备等条件保障的情况，在学科建设、人才引进、团队建设、研究生培养指标、自主选题研究等方面给予优先支持的情况。

实验室在运行经费、办公场地、人才引进、评价机制、学术活动、国内外协作等方面都得到依托单位山东大学的全力支持。另外，山东大学给予实验室独立的建制、充分的人事和财务自主权，使研究人员能够把精力集中在科学研究和实验室发展上，为将本实验室建设成为有重要国际影响的研究平台，稳固我国在国际密码与信息安全重要地位做出巨大贡献。

3、仪器设备

简述本年度实验室大型仪器设备的使用、开放共享情况，研制新设备和升级改造旧设备等方面的情况。

实验室拥有高性能服务器 IBM X3950 和 GPU 服务器，由于本实验室科研计算任务繁重，两台服务器常年 24 小时运行。随着实验室承担的科研任务的加重，两台服务器已经难以满足计算需求，本年度实验室新增华为刀片服务器（含 11 片），解决了计算资源短缺的问题。

六、审核意见

1、实验室负责人意见

实验室承诺所填内容属实，数据准确可靠。

数据审核人:
实验室主任:
（单位公章）
年　　月　　日

2、依托高校意见

依托单位年度考核意见:
（需明确是否通过本年度考核，并提及下一步对实验室的支持。）

依托单位负责人签字:
（单位公章）
年　　月　　日