“物理攻击与安全评测”研讨会（PANDA2014）会议通知

(www.pandacourse.com)

2014 年 PANDA 将于 10 月 20-24 日在山东济南举行。本次 PANDA 研讨会由山东大学计算机学院、山东华芯半导体和深圳纽创信安科技开发公司共同主办。PANDA 会议旨在促进国内外学术交流、推动科研和产业互动。PANDA 每年邀请国内外一线专家作专题报告，课程内容上力求覆盖本领域的前沿科研成果和企业的实际需求。本研讨会所有报告由程序委员会确定，不设论文投稿和海报环节。

现将研讨会的有关事项通知如下：

一、主办单位

山东大学计算机科学与技术学院、山东省华芯半导体、深圳市纽创信安科技开发有限公司

二、会议时间

报到时间：2014 年 10 月 19 日晚 17:00-21:00

会议时间：2014 年 10 月 20 日至 24 日

三、会议地点

山东省济南市齐鲁软件园 A415 会议室

四、参会人员

高等院校、科研院所从事密码芯片及相关专业的专家、学者、科技工作者，信息安全专业和密码专业的在读博士生、研究生，从事密码产品开发和应用的企事业技术人员。

五、注册费

全职在校学生 3000 元/人，大学教师或研究所职员 4000 元/人，企业职员 6000 元/人。

注册费含会议相关的资料费、餐费、茶点、宴会等费用。

六、Riscure 优秀学生奖学金（2 位）

作为 PANDA 的赞助商，Riscure 将提供两份优秀学生奖学金。Riscure 将为奖学金获得者报销注册费、差旅及住宿费用。所有高校、科研机构的全职硕士、博士生都可以申请。请在 10 月 11 日（北京时间 23:59）前将**学生证照片、个人简历和研究方向（英语）、申请理由（英语，并附带导师签字）**发送到以下邮件：

fanjunfeng@gmail.com (抄送：marzec@riscure.com)

Riscure 将在北京时间 2014 年 10 月 15 日前通过邮件通知遴选结果。Riscure 对奖学金事务具有最终解释权。

七、相关事项

1. 因受场地所限，名额有限，先到先得。请于 **2014** 年 **10** 月 **16** 日前(含)完成在线注册。

2. 注册费可缴纳可选择以下方式之一：

（1）银行转账汇款（请在 2014 年 10 月 18 日之前（含）汇出）

账 户 名：深圳市纽创信安科技开发有限公司

开 户 行：中国工商银行深圳蛇口支行

帐 号：4000020209200537760

附 言：PANDA2014 + 姓名

（2）现场缴费（只限于 2014 年 10 月 17 日之后的注册人员）：由于涉及到会议发票的开具，现场缴纳费用将多收取 100 元的手续费，交款方式为现金。

3. 会议酒店：济南东海山庄（顺峰酒店）、济南大卫国际酒店、7 天连锁（国际会展 2 店）其他住宿信息详见暑期班主页。

4. 最新信息请关注暑期班网址： http://www.pandacourse.com

联系人：马晖　　联系电话：010-82546562 – 8060

5. 关于会议最新信息，请参考官方微信：**pandacourse**

PANDA2014 组委会

2014 年 10 月 3 日

附一、PANDA 2014 组委会和赞助商

大会顾问

- **鲍丰**，华为安全与隐私研究所所长 (新加坡)
- **陈弘毅**，清华大学微电子所
- Ingrid Verbauwhede, KU Leuven (比利时)
- Marc Witteman, Riscure (荷兰)

大会主席

- **徐秋亮**，山东大学
- **邢广军**，山东华芯半导体

程序委员会

- **樊俊锋（主席）**，深圳市纽创信安科技开发有限公司(OSR)
- **张锐（主席）**，中国科学院
- **周永彬**，中国科学院
- Benedikt Gierlichs，天主教鲁汶大学（比利时）

赞助单位

- Riscure (荷兰)
- 山东华芯半导体
- 深圳市纽创信安科技开发有限公司

附二、PANDA 2014 主讲人

Marc Witteman, CTO

Riscure (荷兰)

Marc Witteman 是荷兰 Riscure 创始人兼 CTO，并将 Riscure 发展成为全球密码芯片检测设备的第一品牌。他在信息安全行业有超过 20 年的经验，参与过的项目包括移动通信、金融支付系统、身份认证、付费电视、电子护照等产品，他还是多篇关于智能卡和嵌入式系统安全的论文作者。作为一个资深安全测评员，他开发了多个用于安全性检测的软硬件系统，包括后来成为 Riscure 产品的 Inspector。他还是用于逻辑测试的 JCworkBench 的作者。

Marc Witteman 热心参与信息安全行业的交流和培训，具有丰富的培训经验。他参加了 2013 年 PANDA 研讨会并作专题报告。

Benedikt Gierlichs，博士

COSIC, KU Leuven（比利时）

Benedikt Gierlichs 博士毕业于鲁汶大学，师从于著名密码学家、前世界密码协会主席 Bart Preneel 教授。他的主要研究兴趣是旁路分析和错误注入分析及其防护。他是 25 篇学术论文的作者，包含 CHES 文章 7 篇、CT-RSA 文章 3 篇、ASIACRYPT 文章 2 篇、Journal of Cryptology 一篇。他是互信息分析（Mutual Information Analysis）的发明人。

金意儿，博士

University of Central Florida (美国)

金意儿教授毕业于耶鲁大学，目前任职于弗罗里达 UCF 大学。他的主要研究兴趣是硬件木马的设计和检测、可信嵌入式系统和硬件 IP 保护。他首先提出使用局部旁路信息监测硬件木马的方法学、第一个在产品使用阶段的安全性评估框架和第一个自带证明的硬件 IP 保护策

略。他对无联网和可穿戴电子的安全也有浓厚的兴趣。2014 年，金意儿教授应邀在黑帽大会上作专题报告。

石竑松，博士

中国信息安全测评中心

石竑松博士毕业于电子科技大学，研究方向为密码学和理论计算机科学，2007-2009 在加拿大 Calgary 大学 Rei Safavi-Naini 教授处（iCIS 实验室）学习，目前在中国信息安全测评中心从事密码产品安全评估工作，主要研究随机数发生器、侧信道安全及 Leakage-resilient cryptography。他在《Designs, Codes and Cryptography》、《IEEE Transactions on Information Theory》、AsiaCCS、ISIT、CANS 等期刊和会议上发表论文十余篇，在国际 Common Criteria 年会上进行了 2 次特邀报告，是 Eurocrypt （2009, 2010），Crypto （2009，2011）， ICITS 2008 等会议及 IEEE IT 和 JIS 等期刊的审稿人，并参与制定了 3 项信息安全国家标准。

Stefan Tillich，CTO

Yagoba (奥地利)

Stefan Tillich 博士毕业于奥地利 Graz 大学 ,主要研究兴趣是密码芯片设计。博士毕业后，他在英国布里斯托大学从事博士后研究，师从著名密码学家 Nigel Smart 教授，主要研究侧信道攻击技术。Stefan Tillich 博士于 2013 年和另外两位 Graz 大学校友共同创立了 Yagoba，并担任 CTO。Yagoba 致力于高性能、高安全 Java Card Applet 设计。

樊俊锋，CEO

Open Security Research (中国)

樊俊锋博士毕业于比利时鲁汶大学，他的主要研究课题为密码芯片安全，包括高性能密码

芯片、低功耗椭圆曲线密码（ECC）核和抗物理攻击密码芯片设计。他在国际期刊上发表论文 6 篇，学术著作 2 本（章节），国际学术会议论文 20 余篇，包括 CHES 论文 5 篇。他于 2014 年初在深圳创立了纽创信安开放安全技术研究所（Open Security Research, OSR），致力于密码芯片的攻击和防护新技术的研究。

Viktor Fischer，博士

Jean Monnet University Saint-Etienne (法国)

Viktor Fischer 博士任教于法国 Saint-Etienne 大学，主要研究兴趣为密码芯片设计和分析。他对不同平台、不同原理的随机数发生器做了长期、系统的研究，在 CHES、FPL 等国际会议上发表文章近 30 篇。他也应邀在 2014 的 CHES 会议上作随机数设计培训。

Frederik Vercauteren，博士

COSIC, KU Leuven（比利时）

Frederik Vercauteren 博士任教于比利时鲁汶大学，主要研究兴趣为密码数学理论。他在椭圆曲线和超椭圆曲线、线性对（Pairing）和全同态密码领域都有重要成果。特别是在全同态密码技术方面，他在软硬件性能优化方面都有国际先进的研究进展。

附三、PANDA 2014 主要内容

- 安全芯片分析和测评：新技术和新挑战
- 模板攻击及其防护
  a. 模板攻击的基本思想、常用模板攻击技术、最新进展
- 高阶 DPA 攻击及防护
  a. 高阶 DPA 的基本思想、高阶 DPA 技术的应用、最新进展
- 硬件木马设计及检测
  a. 硬件木马的设计、硬件木马的检测、最新发展
- 高性能、高安全 Java Card Applet (JCA)设计
  a. JCA 的设计基础、JCA 性能优化策略、JCA 抗攻击设计方法
- 随机数发生器的设计和检测
  a. 随机数发生器原理、欧洲和美国评测标准、最新攻击技术
- 全同态密码技术
  a. 全同态技术的快速并行计算方法、基于 FPGA 的快速实现