

## “物理攻击与安全评测”研讨会（PANDA2014）会议通知

[www.pandacourse.com](http://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、深圳纽创信安科技开发公司和山东华芯半导体有限公司共同主办。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、深圳市纽创信安科技开发有限公司、山东华芯半导体有限公司

### 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](mailto:fanjunfeng@gmail.com)（抄送：[marzec@riscure.com](mailto: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发展有限公司

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**



## 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
- 张锐, 中国科学院

### 程序委员会

- 樊俊锋 (主席), 深圳市纽创信安科技发展有限公司(OSR)
- 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)
- 深圳市纽创信安科技发展有限公司
- 山东华芯半导体有限公司

## 附二、PANDA 2014 主讲人（部分）

### 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，目前任职于佛罗里达 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。

## 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 会议日程

| 10月19日(周日)    |       |  |
|---------------|-------|--|
| 17:00 - 21:00 | 报到、注册 |  |

| 10月20日（周一）    |                 |               |
|---------------|-----------------|---------------|
| 08:45 - 09:00 | 欢迎辞             | 大会主席、程序委员会主席  |
| 09:00 - 09:50 | 特邀报告            | Marc Witteman |
| 09:50 - 10:30 | 银联卡安全性检测        | 彭乾            |
| 10:30 - 10:50 | 茶歇              |               |
| 10:50 - 11:40 | 密钥产品的安全评估-方法与问题 | 石竑松           |
| 12:10 - 14:00 | 午餐              |               |
| 14:00 - 14:50 | 硬件木马设计与检测-S1    | 金意儿           |
| 14:50 - 15:40 | 硬件木马设计与检测-S2    | 金意儿           |
| 15:40 - 16:10 | 茶歇              |               |
| 16:10 - 17:00 | 硬件木马设计与检测-S3    | 金意儿           |

| 10月21日（周二）    |  |                      |
|---------------|--|----------------------|
| 09:00 - 09:50 | Lattice-based Attack on ECDSA                    | Frederik Vercauteren |
| 09:50 - 10:40 | Smart Nest Thermostat - A Smart Spy in Your Home | 金意儿                  |
| 10:40 - 11:00 | 茶歇   |                      |
| 11:40 - 11:50 | Java Card Applet - S1                            | Stefan Tillich       |
| 12:10 - 14:00 | 午餐   |                      |
| 14:00 - 14:50 | Java Card Applet - S2                            | Stefan Tillich       |
| 14:50 - 15:40 | Java Card Applet - S3                            | Stefan Tillich       |
| 15:40 - 16:10 | 茶歇   |                      |
| 16:10 - 17:00 | Java Card Applet - S4                            | Stefan Tillich       |
| 18:00 - 21:00 | Riscure HACTON活动                                 | Riscure              |

| 10月22日（周三）    |                       |                    |
|---------------|-----------------------|--------------------|
| 09:00 - 09:50 | Java Card Applet - S5 | Stefan Tillich     |
| 09:50 - 10:40 | Java Card Applet - S6 | Stefan Tillich     |
| 10:40 - 11:00 | 茶歇                    |                    |
| 11:40 - 11:50 | Template Attacks - S1 | Benedikt Gierlichs |

|               |                       |                    |
|---------------|-----------------------|--------------------|
| 12:10 - 14:00 | 午餐                    |                    |
| 14:00 - 14:50 | Template Attacks - S2 | Benedikt Gierlichs |
| 14:50 - 15:40 | Template Attacks - S3 | Benedikt Gierlichs |
| 15:40 - 16:10 | 茶歇                    |                    |
| 16:10 - 17:00 | Template Attacks - S4 | Benedikt Gierlichs |
| 18:00 - 21:00 | 会议晚餐                  |                    |

| 10月23日（周四）    |                     |                    |
|---------------|---------------------|--------------------|
| 09:00 - 09:50 | High Order DPA - S1 | Benedikt Gierlichs |
| 09:50 - 10:40 | High Order DPA - S2 | Benedikt Gierlichs |
| 10:40 - 11:00 | 茶歇                  |                    |
| 11:40 - 11:50 | High Order DPA - S3 | Benedikt Gierlichs |
| 12:10 - 14:00 | 午餐                  |                    |
| 14:00 - 17:00 | Excursion           |                    |

| 10月24日（周五）    |  |                      |
|---------------|--|----------------------|
| 09:00 - 09:50 | Fully Homomorphic Encryption (全同态密码技术) | Frederik Vercauteren |
| 09:50 - 10:40 | Random Number Generators - S1          | Viktor Fischer       |
| 10:40 - 11:00 | 茶歇                                     |                      |
| 11:40 - 11:50 | Random Number Generators - S2          | Viktor Fischer       |
| 12:10 - 14:00 | 午餐                                     |                      |
| 14:00 - 14:50 | Random Number Generators - S3          | Viktor Fischer       |
| 14:50 - 15:40 | Random Number Generators - S4          | Viktor Fischer       |
| 15:40 - 16:00 | 茶歇                                     |                      |
| 16:00 - 16:50 | Random Number Generators - S5          | Viktor Fischer       |
| 16:50 - 17:00 | 总结、再见                                  |                      |