

**物理攻击与安全评测技术研讨会 (PANDA’14)**

**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

**会议时间**： 2014年10月20 – 24日

**会议地点:**  山东∙济南

**一、关于PANDA 研讨会**

信息技术越来越广泛地影响我们生活，信息安全的重要性也日益凸显，而密码芯片则是信息安全系统的核心组件。密码芯片行业的攻击技术发展十分迅速，对芯片设计和安全性检测都带来了很大的挑战。对于此，只能通过积极学习国际先进技术、深度参与企业与高校研发合作、共同制定业界安全性检测标准，才能保持我国的安全产品技术的先进性和自主性。

PANDA会议的宗旨是促进国内外学术交流、推动科研和产业互动。在安全芯片设计、分析和检测方面，欧美起步最早，目前技术最先进。为此，我们邀请全世界公认的一线专家来华作专题报告，推动我国在该领域快速进步。在课程内容上，我们要求同时覆盖科研领域的**前沿技术**和我国企业的**实际需求**。在参与对象上，我们邀请学术机构、芯片设计企业和安全性评测机构共同参与。

2013年9月，第一届PANDA在成都举行。我们邀请到了前世界密码协会主席Bart Preneel、Riscure创始人兼CTO Marc Witteman等多名专家来华授课，吸引了学术界、企业界和检测单位等共50多人参会。参会企业包括如下单位。



**二、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](http://homes.esat.kuleuven.be/~iverbauw/), KU Leuven (比利时)
* [Marc Witteman](http://www.linkedin.com/pub/marc-witteman/27/288/261), 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
* **张锐（主席）**，中国科学院
* **周永彬，**中国科学院
* **张翌维，**国民技术股份有限公司
* **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

**三、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。

# 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。他率先提出使用多项式-整数混合模乘算法降低了基于BN曲线的线性对（Pairing）的运算复杂度。使用该算法，他设计了当时世界上最快的Pairing协处理器。他还设计了面向受限设备的超低功耗的ECC芯片，对ECC的抗攻击设计技术进行了系统化研究，提出了一系列低成本检错技术。与Gierlichs和Vercauteren联合设计了的基于无穷远点的攻击方法。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。

**四、PANDA 2014主要内容**

PANDA 2014为期5天，在顾问团的指导下，特拟定以下几个方向。

* **安全芯片分析和测评：新技术和新挑战**
* **模板攻击及其防护**
  1. 模板攻击的基本思想
  2. 常用模板攻击技术
  3. 模板攻击研究的最新进展
* **高阶DPA攻击及防护**
  1. 高阶DPA的基本思想
  2. 高阶DPA技术的应用
  3. 高阶DPA的最新进展
* **硬件木马设计及检测**
  1. 硬件木马的设计
  2. 硬件木马的检测
  3. 硬件木马技术的发展
* **高性能、高安全Java Card Applet设计**
  1. JCA的设计基础
  2. JCA性能优化策略
  3. JCA抗攻击设计方法
* **随机数发生器的设计和检测**
  1. 随机数发生器原理及再思考
  2. 真随机数发生器的攻击和评测

**五、PANDA 2014注册**

会议注册、交通、住宿等信息请参见PANDA官网:

[www.pandacourse.com](http://www.pandacourse.com)

关于会议最新信息，请参考官方微信：**pandacourse**

