“物理攻击与安全评测”研讨会（PANDA2015）会议通知

(www.pandacourse.com)

2015 年 PANDA 会议将于 8 月 26-29 日在深圳举行。本次 PANDA 研讨会由中国密码学会芯片专业委员会指导，由深圳大学、中国科学院信息工程研究所和深圳市纽创信安科技开发有限公司联合主办，由佛山芯珠微电子有限公司和济南钮信安全技术有限公司共同协办。PANDA 会议旨在促进国内外学术交流、推动科研和产业界互动。PANDA2015 邀请了 10 位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、指导单位

中国密码学会芯片专业委员会

二、主办单位

深圳大学

中国科学院信息工程研究所

深圳市纽创信安科技开发有限公司

三、协办单位

佛山芯珠微电子有限公司

济南钮信安全技术有限公司

四、会议时间

报到时间：2015 年 8 月 25 日 16:00-21:00

会议时间：2015 年 8 月 26 日至 29 日

五、会议地点

深圳大学科技楼第三报告厅

六、参会人员

从事 POS 机、移动支付、生物识别等产品的企业从业人员；

从事密码芯片研发、密码芯片测试的技术人员；

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硕士及博士研究生。

七、注册费

本次会议分为两个部分：支付系统安全和芯片安全。企业参会人员可选择只参加支付系统安全部分，也可两个都选择。

- 企业参会人员仅参加支付安全部分，注册费为 **2000** 元/人，课程安排在 26 日全天和 27 日上午；
- 企业参会人员参加整个会议，注册费为 **4000** 元/人；
- 高校教师和研究所职员注册费为 **2500** 元/人；
- 全职在校学生注册费为 **1500** 元/人，需发送在学证明（如学生证扫描件）至大会邮箱 pandacourse@gmail.com。

注册费含会议相关的资料费、午餐、茶点、宴会等费用。

八、相关事项

1.因受场地所限，名额有限，先到先得。请于 **2015 年 8 月 20 日**前(含 20 日)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 2015 年 8 月 20 日之前（含 20 日）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 ：PANDA2015 + 姓名

（2）现场缴费（只限于 2015 年 8 月 20 日之后的注册人员）：由于涉及到会议发票的开具，现场缴费将多收取 100 元的手续费，缴款方式只能为现金，发票领取方式为会后邮寄。

3. 住宿：详见主页。

4. 最新信息请关注主页： http://www.pandacourse.com

联系人：赵鹏　　联系电话： 0755-86950263

5. 关于会议最新信息，请参考官方微信：**pandacourse**

PANDA 2015 组委会

2015 年 7 月 31 日

附一、PANDA 2015 组委会和赞助商

大会顾问

- **陈弘毅**, 清华大学
- **Benedikt Gierlichs,** 天主教鲁汶大学（比利时）
- **Marc Witteman**，Riscure（荷兰）
- **熊晓明**, 广州国家现代服务业集成电路设计产业化基地

大会主席

- **张锐**，中国科学院
- **喻建平**，深圳大学

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)
- **白国强（主席）**，清华大学
- **张勇**，深圳大学
- **周永彬**，中国科学院
- **吴震**，成都信息工程大学
- **王安**，北京理工大学
- **李阳**，南京邮电大学

组委会

- **马晖**，中国科学院
- **赵鹏**，深圳市纽创信安科技开发有限公司

赞助单位

- NXP Semiconductors
- 深圳市纽创信安科技开发有限公司
- 中国科学院信息工程研究所信息安全国家重点实验室

附二、PANDA 2015 主讲人（部分）

Speakers	Affiliation	Bio
Bart Preneel	COSIC, KU Leuven, Belgium	Bart Preneel is full professor at the KU Leuven where he heads the COSIC research group which has 60 members. He has authored more than 400 scientific publications and is inventor of 4 patents. His main research interests are cryptography, information security and privacy and he frequently consults on these topics. Bart Preneel has participated to more than 30 international research projects sponsored by the European Commission, for five of these as project manager. He has served as panel member for several research funding agencies including the European Research Council. He is president of the IACR (International Association for Cryptologic Research) and a member of the Permanent Stakeholders group of ENISA.
Michael Ward	Mastercard, UK	Michael Ward works in the Chip Centre of Excellence Product Security department within MasterCard Worldwide‘s Advanced Payments group. He provides security expertise in areas such as cryptography and key management for chip card applications and is chairman of the EMVCo Security Working Group. He participates in various international standards bodies including ISO/IEC JTC 1 /SC 27/WG 2 Information Technology - Security Techniques and Mechanisms, ISO TC 68 Financial Services, and the European Payments Council Security Payments Task Force. Before joining MasterCard he was an employee at APACS (the Association for Payment Clearing Services) in the UK where he was involved with the UK migration to chip card technology. He has a degree in mathematics from Oxford University and a Ph.D. from Royal Holloway, London University.
Peter Fillmore	Independent researcher	Peter Fillmore is a payment security expert with extensive experience in the design and certification of PCI PTS approved payment terminals. Peter has been involved with all types of terminal design - from simple swipe mechanisms to complex unattended systems. Previously he has spoken at Blackhat USA, Syscan and Breakpoint security conferences on contactless payment security implementations. His research work has been covered by all forms of international and national media including TV, radio and newspapers. Peter is interested in real world security systems and novel ways of breaking them.

Olivier Rioul	Telecom-ParisTech, France	Olivier Rioul is a currently an associate professor at Télécom ParisTech. His research interests include joint source-channel coding and information theory. Olivier Rioul was born in Strasbourg, France on July 4, 1964. He received diplomas in Electrical Engineering from the Ecole Polytechnique, Palaiseau, France, and from Telecom University, Paris, in 1987 and 1989, respectively. From 1989 to 1994, he was with the Centre National d'Etudes des Télécommunications (CNET), Issy-les-Moulineaux, France, where he worked on wavelet theory and image compression.
Benedikt Gierlichs	COSIC, KU Leuven, Belgium	Benedikt Gierlichs is currently a post-doctoral fellow with the Funds for Scientific Research Flanders (Belgium). His research focuses on the (physical) security of embedded devices, in particular side-channel analysis, fault analysis and countermeasures. He is (co-)author of more than 25 scientific publications in international, peer-reviewed conferences and journals. Dr. Benedikt Gierlichs joined the COSIC research group at KU Leuven (Belgium) as a PhD student in 2006. He obtained a PhD in electrical engineering with his thesis on "Statistical and Information-Theoretic Methods for Power Analysis on Embedded Cryptography" in 2011. Prior to joining COSIC, Benedikt Gierlichs studied IT-security engineering at the university of Bochum and obtained an MSc in 2006. Further, he completed a long-term internship at the Security Technologies department of Gemplus (now part of Gemalto).
Frederik Vercauteren	COSIC, KU Leuven, Belgium	Frederik Vercauteren received the M.Sc. degree in computer science, the M.Sc. degree in pure mathematics, and the Ph.D. degree in electrical engineering from the Katholieke Universiteit Leuven, Belgium. He is currently a Post-doctoral Fellow of the Research Foundation-Flanders (FWO) at the Department of Electrical Engineering, Katholieke Universiteit Leuven, Belgium. Previously, he held a lecturer position at the Department of Computer Science, University of Bristol, U.K. His current research interests include applications of computational number theory and arithmetic geometry in cryptography.
Yang Li	Nanjing University of Aeronautics and Astronautics, China	Yang Li received the B.E. degree in electronic and information engineering from Harbin Engineering University, Harbin, China, in 2008, the M.E. degree in information and communication engineering and the Ph.D. degree in faculty of informatics from the University of Electro-Communications, Tokyo, Japan, in 2011 and 2012, respectively. He is currently an associated professor in College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, China. His current research interests include security evaluation and improvement for cryptographic hardware and embedded systems.

Huiyun Li	Chinese Academy of Sciences, China	Huiyun Li obtained her PhD degree from Cambridge University, UK in 2006. She has been working with Shenzhen Institute of Advanced Technologies, China since 2006 and is the vice director of the Automotive Electronics Research Center. Her research interests include cryptographic module/IC design, evaluation and test, as well as power electronics and system in package (SIP) test. She has published 1 book and over 30 papers on international journals and conferences. She is the principle investigator (PI) of projects supported by China National High-tech 863 plan and National Science Foundation of China etc. She is the peer reviewer of multiple international academic journals and conference proceedings. She was awarded as Cambridge Overseas Trust Scholar (2003) and Outstanding Talent of Shenzhen (2009).
Qiang Xu	Chinese University of Hong Kong, Hong Kong	Qiang Xu is an Associate Professor of Computer Science & Engineering at The Chinese University of Hong Kong. He received his B.E. and M.E. degrees in Telecommunication Engineering from Beijing University of Posts & Telecommunications, China, in 1997 and 2000, respectively. After working at a start-up integrated circuit design house for one and a half years, he continued his graduate study and received his Ph.D. degree in Electrical & Computer Engineering from McMaster University, Canada, in 2005, and then joined CUHK. Dr. Xu leads the CUhk REliable computing laboratory (CURE Lab.). His research interests include fault-tolerant computing, trusted computing and accelerated computing for finance and biomedical applications. He received the Best Paper Award in 2004 IEEE/ACM Design, Automation and Test in Europe (DATE). He has four other papers nominated for best paper award at prestigious conferences. Dr. Xu is currently serving as an associate editor for IEEE Design and Test of Computers. He has also served as technical program committee members for a number of conferences on VLSI design and testing, including DAC, ITC, ICCAD, and DATE.
Yu Yu	Shanghai JiaoTong University	Yu Yu is currently a research professor at Shanghai Jiao Tong University. He obtained his BSc from Fudan University in 2003, and his PhD from Nanyang Technological University in 2006. He worked as a researcher at the ICT security lab at T-Systems Singapore from 2006 to 2008, and as a postdoctoral researcher at the UCL Crypto Group from 2008-2010. After returned to China, he was employed by East China Normal University (2011-2012) and Tsinghua University (2012-2014). His research interests include foundations of cryptography, pseudorandomness, and leakage-resilient cryptography. He has a dozen of publications at major venues such as CRYPTO, CCS, TCC, Asiacrypt, and CHES.

附三、PANDA 2015 会议日程

8月25日(周二)	
16:00 - 21:00	报到、注册

8月26日（周三）		
Section 1: Payment Security		
09:15 - 10:00	Challenges and trends in EMV payment system - 1	Michael Ward
10:20 -11:00	Challenges and trends in EMV payment system - 2	Michael Ward
11:00 -11:20	茶歇	
11:20 - 12:00	Challenges and trends in EMV payment system - 3	Michael Ward
12:10 - 14:00	午餐	
14:00 - 14:40	PCI PTS security - 1	Peter Fillmore
15:00 - 15:40	PCI PTS security - 2	Peter Fillmore
15:40 - 16:00	茶歇	
16:00 –16:40	构建立体式风险评估体系应对应用安全挑战	Huiya Yao
17:00 –18:00	Q & A	

8月27日（周四）		
09:15 -10:00	Cryptography in payment	Bart Preneel
10:20 - 11:00	FIDO protocols and implementation	Frederik Vercauteren
11:00 - 11:20	茶歇	
11:20 - 12:00	Bitcoin security	Frederik Vercauteren
12:10 - 14:00	午餐	
Section 2: Design and analysis of cryptographic chips		
14:00 - 14:40	Introduction to power analysis	Huiyun Li
15:00 - 15:40	Evaluation and Improvement of Generic-Emulating DPA Attacks	Yu Yu
15:40 - 16:00	茶歇	
16:00 - 16:40	Introduction to Fault-sensitivity analysis	Yang Li
17:00 - 18:00	Q & A	
18:10 - 20:00	会议晚餐	

8月28日（周五）		
09:15 -10:00	Introduction to white-box cryptography	Bart Preneel
10:20 - 11:00	Privacy challenges for biometrics authentication	Bart Preneel
11:00 - 11:20	茶歇	
11:20 - 12:00	Hardware security in EMV payment system	Michael Ward
12:10 - 14:00	午餐	
14:00 - 14:40	Side-Channel Analysis: A Mathematician's Viewpoint	Olivier Rioul
15:00 - 15:40	Side-Channel Analysis: A Mathematician's Viewpoint	Olivier Rioul
15:40 - 16:00	茶歇	
16:00 - 16:40	Side-Channel Analysis: A Mathematician's Viewpoint	Olivier Rioul
17:00 - 18:00	Q & A	

8月29日（周六）		
09:15 -10:00	Threshold implementation	Benedikt Gierlichs
10:20 - 11:00	Inner product masking	Benedikt Gierlichs
11:00 - 11:20	茶歇	
11:20 - 12:00	Attacking 1GHz ARM-Cortex A8	Benedikt Gierlichs
12:10 - 14:00	午餐	
14:00 - 14:40	Hardware Trojan	Qiang Xu
15:00 - 15:40	Hardware Trojan	Qiang Xu
15:40 - 16:00	茶歇	
16:00 - 16:40	Student presentations & discussion	
17:00 - 18:00	Closing remarks	

8月30日（周日）	
10:00 - 18:00	Excursion