目　录

2009 国际密码年会综述

罗　岚

lanneverlose@yahoo.com.cn

摘要：本文是对 2009 年 IACR 直接组织的国际密码年会的综述，仍然包括了一些国际黑帽大会。由于 SHA3 进入第二轮，09 年的密码学界在下半年被 NIST 左右，因为把做摘要的明文背景和 SHA3 算法直接做运算，HASH 就可以看做是流密码。因此，虽然到目前为止美国还没有公开的流密码设计征集，这些设计的原则和一些细致的走向是整个对称密码都可以使用的。对理论模型和硬件攻击也是这一年的看点，的确，密码很大成分的吸引力在应用。
关键字：2009 国际密码年会，2009 黑帽大会，SHA3 第二轮

2009年2月22日到25日，**FSE2009**在比利时鲁汶召开，由 Katholieke Universiteit Leuven 的COSIC研究组主办，同时NIST召开了SHA3的第一次候选算法大会；**PKC 2009** 收到112篇文章，录用了28篇，3月在美国Irvine召开；**Euro2009** 于4月在德国 Cologne 召开，会议主席是德国的 Alexander May。收到148篇投稿，33篇文章被录用；**RSA2009**会议在4月份召开，地点是美国圣弗兰西斯科，从93份投稿里录用了31篇文章，会议执行主席是德国的 Marc Fischlin； **CHES2009**在9月6——9日于瑞士举办，包括3个特邀报告和从148份投稿中选出的29篇文章；**2009亚密会**12月6日到10日在日本东京召开；**第29届美密会**于8月16号至20号在加里弗利亚大学举行，从213篇投稿里收录了三十八篇文章；**2009美国黑帽大会**于7月25日—30日在拉斯维加斯举行；**2009欧洲黑帽大会**于4月14日——17日在阿姆斯特丹举行。2009 IACR 组织的国际密码会议论文由LNCS出版，为EI级别，编辑主要为英国，美国，瑞士，以色列，印度，德国，芬兰。

一、安全、证明和模型

Euro2009 安全、证明和模型的文章包括：Mihir Bellare, Dennis Hofheinz, and Scott Yilek 写的 “在选择公开的条件下加密和承诺安全的可能和不可能结果”。 Divesh Aggarwal and Ueli Maurer 写的“分解通常意义下的 RSA 是与因式分解同等难度”。Vipul Goyal and Amit Sahai 写的“重置安全计算”。Chi-Jen Lu 写的“在密码学归约条件下的安全丢失”。Yevgeniy Dodis, Thomas Ristenpart, and Thomas Shrimpton 写的“实际应用 Merkle-Damg˚ard 的补丁”。Eike Kiltz and Krzysztof Pietrzak 写的“在标准模型下的基于底码的加密体制的安全或为什么不能证明 OAEP 安全”。 Mihir Bellare and Thomas Ristenpart 写的“没有人为中止的仿真：对 Waters’ IBE 体制的简单证明和提高具体安全”。Jan Camenisch, Aggelos Kiayias, and Moti Yung 写的“一个简单的普通 Schnorr 证明”。**RSA2009 会议（协议分析）**：Stefan Lucks, Andreas Schuler, Erik Tews, Ralf-Philipp Weinmann, and Matthias Wenzel “攻击 DECT 认证体制”； Andrew Y. Lindell 写的“基于比较的密钥交换和在兰牙 2.1 版本里的数字比较模型的安全”； Mihir Bellare, Shanshan Duan, and Adriana Palacio 写的“密钥隔离和在公钥信道上的弹性回归”；Manoj Prabhakaran and Rui Xue 写的“隐藏子集分析”；Andrew Y. Lindell 写的“删掉的两方计算动态安全”； Tomas Toft 写的“秘密共享值的固定圈、几乎线性比特分

解”；Andrew Y. Lindell 写的“对同时构造的本地顺序没有帮助”； Matthew Franklin, Mark Gondree, and Payman Mohassel 写的“对最长共同序列的有效通信秘密协议”；Giuseppe Ateniese, Karyn Benson, and Susan Hohenberger 写的“秘密密钥范式重新加密”；Man Ho Au, Patrick P. Tsang, Willy Susilo, and Yi Mu 写的“对 DDH 群的动态广泛聚积和他们在基于属性的匿名认证体制的应用”； Tomas Toft 写的“秘密共享值的固定圈、几乎线性比特分解”；Andrew Y. Lindell 写的“对同时构造的本地顺序没有帮助”； **PKC 2009 应用和协议**：Dan Boneh, David Freeman, Jonathan Katz, and Brent Waters 写的“签名一个线性子空间：对网络编码的签名体制”；Pascal Junod, Alexandre Karlov, and Arjen K. Lenstra 写的“提高 Boneh- Franklin 反叛追踪体制”；M. Choudary Gorantla, Colin Boyd, and Juan Manuel Gonz′alez Nieto 写的“基于组密钥加密模型构造密钥折中假冒模型攻击”；Aggelos Kiayias and Hong-Sheng Zhou 写的“使用删除证据的零知识证明”；Michel Abdalla, Xavier Boyen, C′eline Chevalier, and David Pointcheval 写的“从弱密钥分布公钥密码学”；Ivan Damg˚ard, Martin Geisler, Mikkel Krgaard, and Jesper Buus Nielsen 写的“异步多方计算：理论和实现”；Hossein Ghodosi and Josef Pieprzyk 写的“无所不知攻击者的多方计算”；**第 29 届美密会**：*Rafael Pas, Wei-Lung Dustin Tseng, Douglas Wikstr\"om* 的文章“公共硬币的零知识协议的构造”；*Ronald Cramer and Ivan Damg{\aa}rd* 的文章“零知识协议的分摊复杂度”。**2009 亚密会**：模型和框架 I（组织：Ivan Visconti）Tibor Jager, Jorg Schwenk 写的在普通环模型下的密码假设分析；Hoeteck Wee 写的重新认识随机预言机制下的零知识协议；Masayuki Abe, Miyako Ohkubo 写的对通常可构造的非承诺盲签名的一个框架；模型和框架 II（组织：Serge Vaudenay）Liqun Chen, Paul Morrissey, Nigel P. Smart, Bogdan Wareinschi 写的对于代理难题的安全概念和通常构造；Alexandra Boldyreva, David Cash, Marc Fischlin, Bogdan Warinschi 写的不可扩展单向函数的定义和单向函数。

二、单向函数分析

Euro2009 的：Praveen Gauravaram and Lars R. Knudsen 写的“基于强化数字签名安全的随机单向函数”。Lars R. Knudsen, Florian Mendel, Christian Rechberger, and S en S. Thomsen 写的“MDC-2 的分析”。Xiaoyun Wang, Hongbo Yu, Wei Wang, Haina Zhang, and Tao Zhan 写的“HMAC/NMAC-MD5 和 MD5-MAC 的分析”。Yu Sasaki and Kazumaro Aoki 写的“比穷尽攻击更快的完全 MD5 求取范式”。**FSE2009 会议**收录的文章：基于 HASH 的分组密码重新设计——Martijn Stam，EPFL, Switzerland；对 SHA3 算法的中间人攻击——Dmitry Khovratovich, Ivica Nikolic and Ralf-Philipp Weinmann， University of Luxembourg, Luxembourg；差分分析里的代数技术——Martin Albrecht and Carlos Cid，Royal Holloway, University of London, United Kingdom；LAKE 单向函数簇的碰撞——Ivica Nikolic, Alex Biryukov, Dmitry Khovratovich, Jian Guo, Krystian Matusiewicz, Praveen Gauravaram, San Ling, Josef Pieprzyk and Huaxiong Wang, University of Luxembourg, Luxembourg, Nanyang Technological University, Singapore, Technical University of Denmark, Denmark and Macquaire University, Australia；基于可折叠分组密码算法的超越生日边界安全——Kazuhiko Minematsu, NEC Corporation, Japan；MD6 的差分安全分析——Yevgeniy Dodis, Leonid Reyzin, Ronald L. Rivest and Emily Shen，New York University, USA, Boston University, USA and Massachusetts Institute of Technology, USA。**RSA2009 会议**：Dmitry Khovratovich, Alex Biryukov, and Ivica Nikolic 写的“面向字节的 HASH 函数碰撞快速搜索”；Christophe Petit, Jean-Jacques Quisquater, Jean-Pierre Tillich, and Gilles Z′emor 写的“在 Z′emor-Tillich 单向函数的简单或难得碰撞搜索成分：在等价条件下的新的攻击和归约变化”；**美密会 2009**：*Kazumaro Aoki and*

Yu Sasaki 的文章“减轮 SHA0，SHA1 的中间人范式攻击”；*Thomas Icart* 的文章“怎样 HASH 到椭圆曲线”；**2009 亚密会**：单向函数 I（组织：Josef Pieprzyk）Krystian Matusiewicz, Maria Naya-Plasencia, Ivica Nikolic, Yu Sasaki, Martin Schlaffer 写的全路径压缩函数的边界重构攻击；Mario Lamberger, Florian Mendel, Christian Rechberger, Vincent Rijmen, Martin Schlaffer 写的分别重新构造：完全 WHIRLPOOL 压缩函数的结果；Florian Mendel, Christian Rechberger, Martin Schlaffer 写的 MD5 比弱函数更弱：相关合成攻击；Ryad Benadjila, Olivier Billet, Shay Gueron, Matt Robshaw 写的 Intel 的 AES 指令代码和 SHA3 候选算法；单向函数 II（组织：Tetsu Iwata）Antoine Joux, Stefan Lucks 写的用 3 碰撞提高一般算法；A nja Lehmann, Stefano Tessaro 写的一个单向函数的模块设计：面向设计混合-压缩-混合方法实践；Yusuke Naito, Kazuki Yoneyama, Lei Wang, Kazuo Ohta 写的怎样确认加密体制安全：原始版本 MD 算法仍在使用；**PKC 2009 ，CHES2009** 没有涉及单向函数研究。

三、群和广播加密

Euro2009 包括：Qianhong Wu, Yi Mu, Willy Susilo, Bo Qin, and Josep Domingo-Ferrer 写的“非对称群密钥协议”。Craig Gentry and Brent Waters 写的“在广播加密体制下（用短密文）的适应安全”。Olivier Billet and Duong Hieu Phan 写的“在公共体制的合谋攻击：Pirates 2.0”。**FSE2009 会议**收录的文章：电波估计分析——Thomas Fuhr and Thomas Peyrin，DCSSI, France and Ingenico, France；**RSA2009 会议**：Stefan Lucks, Andreas Schuler, Erik Tews, Ralf-Philipp Weinmann, and Matthias Wenzel “攻击 DECT 认证体制”；Andrew Y. Lindell 写的“基于比较的密钥交换和在兰牙 2.1 版本里的数字比较模型的安全”；**PKC 2009**：多方协议：Michel Abdalla, Xavier Boyen, C′eline Chevalier, and David Pointcheval 写的“从弱密钥分布公钥密码学”；Ivan Damg˚ard, Martin Geisler, Mikkel Krgaard, and Jesper Buus Nielsen 写的“异步多方计算：理论和实现”；Hossein Ghodosi and Josef Pieprzyk 写的“无所不知攻击者的多方计算”。**第 29 届美密会**：*Peter Bro Miltersen, Jesper Buus Nielsen, and Nikos Triandopoulos* 的文章“使用合理密码的加强秘密拍卖”；*Gilad Asharov and Yehuda Lindell* 的文章“在正确和公平合理的秘密共享里的信任效果”；*Vadim Lyubashevsky and Daniele Micciancio* 的文章“距离解码界线：唯一短向量和最小距离难题”。

四、加密体制

Euro2009：Bhavana Kanukurthi and Leonid Reyzin 写的“在不安全的信道上的更近的秘密密钥协议”。Alexandra Boldyreva, Nathan Chenette, Younho Lee, and Adam O’Neill 写的“保阶对称密码体制”。Kan Yasuda 写的“对 MACs, PRFs and PROs 的双管道运算模型：超越生日攻击边界”。**FSE2009 会议**收录的文章：快速而安全的 CBC 型 MAC 算法——Mridul Nandi，National Institute of Standards and Technology, USA；重新设计 IDEA 设计理念——Pascal Junod and Marco Macchetti，University of Applied Sciences Western, Switzerland and Nagracard SA,Switzerland；基于 HASH 的分组密码重新设计——Martijn Stam，EPFL, Switzerland；**RSA2009 会议**：B. Collard and F.-X. Standaert 写的“抗分组密码 PRESENT 的统计饱和曲线”；Thomas Popp, Mario Kirschbaum, and Stefan Mangard 写的“在加强掩码的硬件实践攻击”；Orr Dunkelman and Nathan Keller 写的“CTC2 的分析”；**PKC 2009**：Jun Shao and Zhenfu Cao 写的“没有对子的重新加密 CCA 范式”；Masayuki Abe, Eike Kiltz, and Tatsuaki Okamoto 写的“对任意长度消息的协议安全 CCA 加密”；Sebastiaan de Hoogh, Berry

Schoenmakers, Boris ˇSkori′c, and Jos′e Villegas 写的“同态加密的旋转证明”。**第 29 届美密会：***Ben Morris, Phillip Rogaway, and Till Stegers* 的文章“在小的定义域里怎样加密消息：确定加密和混乱”。CHES2009：Junfeng Fan and Frederik Vercauteren and Ingrid Verbauwhede, Katholieke Universiteit Leuven, Belgium 写的“Barreto-Naehrig 曲线的快速 F_p-算法的密码对”。**2009 亚密会：**加密体制（组织：Rei Safavi-Naini）Julien Cathalo, Benoit Libert, Moti Yung 写的组加密：在标准模型下的非交互观点；Jonathan, Katz, Arkady Yerukhimovich 写的从陷门迭代预测加密的黑盒构造；Tatsuaki Okamoto, Katsuyuki Takashima 写的内积的分级预测加密；Mihir Bellare, Zvika Brakerski, Moni Naor, Thomas Ristenpart, Gil Segev, Hovav Shacham, Scott Yilek 写的保护公钥加密：怎样防止抗坏的随机现象。分组密码（组织：Mitsurui Matsui）：Alex Biryukov, Dmitry Khovratovich AES-192，256 相关密钥分析; Xiaorui Sun, XueJia Lai, 分组密码的独立密钥分析；Peter Gazi, Ueli Maurer 的重新认识迭代加密；小组 2 量子密码（组织：Serge Fehr）：Ivan Damgard, Carolin Lunemann 写的量子源头的随机现象和应用；Louis Savail, Christian Schiaffner, Miroslava Sotakova 写的两方量子密码的阶；Matthieu Finiasa, Nicolas Sendrier 写的：基于编码密码系统的设计安全边界。

五、分析

Euro2009 ：Guilhem Castagnos and Fabien Laguillaumie 写的“二次加密密码体制的安全：最好的分析”。 Itai Dinur and Adi Shamir 写的“对可折叠的黑盒多项式的立方攻击”。Khaled Ouafi and Serge Vaudenay 写的“分解 SQUASH-0”。Dennis Hofheinz and Eike Kiltz 写的“从因式分解实现选择密文安全加密”。 Susan Hohenberger and Brent Waters 写的“在标准假设下实现单向-签名体制”。Jan Camenisch, Nishanth Chandran, and Victor Shoup 写的“选择明文和适时选择密文攻击的一个抗密钥独立公钥加密体制”。**FSE2009：**ISDB 攀登算法（MULTI2）的密码分析——Jean-Philippe Aumasson, Jorge Nakahara Jr. and Pouyan Sepehrdad，FHNW, Windisch, Switzerland and EPFL, Lausanne, Switzerland；减轮 MD6 和 TRIVIUM 的立方测试和密钥恢复攻击——Jean-Philippe Aumasson, Willi Meier, Itai Dinur and Adi Shamir，FHNW, Windisch, Switzerland and The Weizmann Institute, Israe；Tandem-DM 的安全分析——Ewan Fleischmann, Michael Gorski and Stefan Lucks，Bauhaus- University Weimar, Germany；减轮 WHIRLPOOL 和 GROTL 的分析——Florian Mendel, Christian Rechberger, Martin Schl a_er and S_ren S. Thomsen，Graz University of Technology, Austria and Technical University of Denmark, Denmark；MD6 的差分安全分析——Yevgeniy Dodis, Leonid Reyzin, Ronald L. Rivest and Emily Shen，New York University, USA, Boston University, USA and Massachusetts Institute of Technology, USA；对 X-FCSR-256 的一个有效状态恢复攻击——Paul Stankovski, Martin Hell and Thomas Johansson，Lund University, Sweden；一个重构边界攻击：减轮 TAGER 的逆象攻击——Takanori Isobe and Kyoji Shibutani，Sony Corporation, Japan；对 SHA3 算法的中间人攻击——Dmitry Khovratovich, Ivica Nikolic and Ralf-Philipp Weinmann，University of Luxembourg, Luxembourg；差分分析里的代数技术——Martin Albrecht and Carlos Cid，Royal Holloway, University of London, United Kingdom；LAKE 单向函数簇的碰撞——Ivica Nikolic, Alex Biryukov, Dmitry Khovratovich, Jian Guo, Krystian Matusiewicz, Praveen Gauravaram, San Ling, Josef Pieprzyk and Huaxiong Wang, University of Luxembourg, Luxembourg, Nanyang Technological University, Singapore, Technical University of Denmark, Denmark and Macquaire University, Australia；基于可折叠分组密码算法的超越生日边界安全——Kazuhiko Minematsu, NEC Corporation, Japan；MD6 的差分安全分析——Yevgeniy Dodis, Leonid Reyzin, Ronald L. Rivest and Emily Shen，New York University, USA,

Boston University, USA and Massachusetts Institute of Technology, USA 。 **RSA2009 会议：** Mihir Bellare, Shanshan Duan, and Adriana Palacio 写的“密钥隔离和在公钥信道上的弹性回归”；Manoj Prabhakaran and Rui Xue 写的“隐藏子集分析”；Andrew Y. Lindell 写的“删掉的两方计算动态安全”；HASH 函数的碰撞：Dmitry Khovratovich, Alex Biryukov, and Ivica Nikolic 写的“面向字节的 HASH 函数碰撞快速搜索”；Christophe Petit, Jean-Jacques Quisquater, Jean-Pierre Tillich, and Gilles Z'emor 写的“在 Z'emor-Tillich 单向函数的简单或难得碰撞搜索成分：在等价条件下的新的攻击和归约变化”。**第 29 届美密会：** *Zheng Yuan, Wei Wang, Keting Jia, Guangwu Xu, and Xiaoyun Wang* 的文章“基于分组密码的 MAC 的新的生日攻击”；*Alex Biryukov, Dmitry Khovratovich, and Ivica Nikoli\'{c}*的文章“对完整 AES-256 的区分和相关密钥攻击”；*Julia Borghoff, Lars Knudsen, Gregor Leander, and Krystian Matusiewicz* 的文章“C2 的密码分析”。2009 亚密会：密码分析：二次方和三次方（组织：Jun Furukawa）Olivier Billet, Gilles Macario-Rat 写的（Yannick Seurin 发言）平方密码体制的分析；Guilhem Castagnos, Antoine Joux, Fabien Layuillaumie, Phong Q.Nguyen 写的 pq^2 形式的三次方：好的分析；Mathias Herrmann, Alexander May 写的使用分布线性发生器的攻击：为什么我们的输出这么多？

六、边信道攻击

Euro2009： Fran ois-Xavier Standaert, Tal G. Malkin, and Moti Yung 写的“对边信道密钥恢复攻击的”。Krzysztof Pietrzak 写的“一个运算弹性泄露模型”。**FSE2009 会议：** 基于可折叠分组密码算法的超越生日边界安全——Kazuhiko Minematsu, NEC Corporation, Japan；**RSA2009 会议：** Alexandre Berzati, C'ecile Canovas, Jean-Guillaume Dumas, and Louis Goubin 写的“RSA 体制的差错攻击：从左到右实现是脆弱的”；Kazuo Sakiyama, Tatsuya Yagi, and Kazuo Ohta 写的“使用 RSL 抗 AES 原型芯片的差错分析攻击 ”；Thomas Plos 写的“被动 UHF RFID 标签的作为分离电源供应的边信道分析记数测量”；Matthieu Rivain 写的“用双加法幂链进行抗差错分析的安全 RSA”。**CHES2009：** Mathieu Renauld, François-Xavier Standaert and Nicolas Veyrat-Charvillon, UCL, Belgium 写的“对 AES 的代数边信道攻击：为什么 DPA 与时间相关”；Mike Hamburg, Stanford University, USA 写的“使用 Permute 入侵向量的加速 AES 攻击”；Francesco Regazzoni, UCL, Belgium and ALaRI, Switzerland，Alessandro Cevrero, EPFL, Switzerland，François-Xavier Standaert, UCL, Belgium，Stephane Badel, EPFL, Switzerland，Theo Kluter, EPFL, Switzerland，Philip Brisk, EPFL, Switzerland，Yusuf Leblebici, EPFL, Switzerland，Paolo Ienne, EPFL, Switzerland 写的“对抗 DPA 指令集扩展的一个设计流和评估框架”；Anna Inn-Tung Chen, National Taiwan University, Taiwan，Ming-Shing Chen, Academia Sinica, Taiwan，Tien-Ren Chen, Academia Sinica, Taiwan，Chen-Mou Cheng, National Taiwan University, Taiwan，Jintai Ding, University of Cincinnati, USA，Eric Li-Hsiang Kuo, Academia Sinica, Taiwan，Frost Yu-Shuang Li, National Taiwan University, Taiwan，Bo-Yin Yang, Academia Sinica, Taiwan 写的“在现代 X86 处理器上进行多变量 PKCs 的 SSE 实现”；Rajat Subhra Chakraborty, Francis Wolff, Somnath Paul, Christos Papachristou, and Swarup Bhunia, Case Western Reserve University, USA 写的“MERO:对硬件特洛伊的测试方法”；Lang Lin, University of Massachusetts, USA，Markus Kasper, Ruhr University Bochum, Germany，Tim Güneysu, Ruhr University Bochum, Germany，Christof Paar, Ruhr University Bochum, Germany and University of Massachusetts, USA，Wayne Burleson, University of Massachusetts, USA 写的“特洛伊边信道：通过边信道机制的轻型硬件特洛伊”。**2009 亚密会：** 边信道攻击（组织：Goichiro hanaoka）Jean-Sebastien Coron, Avradip Mandal 写的 PSS 抗随意差错攻击是安全的；

Billy Bob Brumley, Risto M. Hakala 写的 Cache 时间模板攻击；Frederik Armknecht, Roel Maes, Ahmad-Reza Sadegh, Berk Sunar, Pim Tuyls 写的基于物理不可克隆函数的记忆弹性泄露加密；Jonathan Katz, Vinod Vaikuntanathan 写的弹性边界泄露的签名体制。

七、曲线

Euro2009 ：Daniel J. Bernstein, Tien-Ren Chen, Chen-Mou Cheng, Tanja Lange, and Bo-Yin Yang 写的“在图卡上的 ECM ”。Christophe Doche, David R. Kohel, and Francesco Sica 写的“对多范围的多方基于双数体制”。Steven D. Galbraith, Xibin Lin, and Michael Scott 写的“在大椭园簇上的快速椭园曲线签名”。Takakazu Satoh 写的“在大特征有限域下的两个 Hyperelliptic 椭园曲线产生”。**第 29 届美密会**：*Thomas Icart* 的文章“怎样 HASH 到椭圆曲线”；*Daniel J. Bernstein* 的文章“一组二进制 EDWARDS 曲线”；**CHES2009**：David Kammler, RWTH Aachen University, Germany，Diandian Zhang, RWTH Aachen University, Germany，Peter Schwabe, Eindhoven University of Technology, Netherlands，Hanno Scharwaechter, RWTH Aachen University, Germany，Markus Langenberg, RWTH Aachen University, Germany，Dominik Auras, RWTH Aachen University, Germany， Gerd Ascheid, RWTH Aachen University, Germany，Rudolf Mathar, RWTH Aachen University, Germany 写的“在 Barreto-Naehrig 曲线上的密码对 ASIP 设计”；Xu Guo, Virginia Tech, USA， Junfeng Fan, Katholieke Universiteit Leuven, Belgium，Patrick Schaumont, Virginia Tech, USA， Ingrid Verbauwhede, Katholieke Universiteit Leuven, Belgium 写的“运算程序和并行 ECC 处理结构：在面积、速度和安全里取舍”。2009 亚密会没有涉及这个方面。

八、数字签名

RSA2009会议：Ee-Chien Chang, Chee Liang Lim, and Jia Xu 写的“使用随机数的可读短签名”； Chong-zhi Gao, Baodian Wei, Dongqing Xie, and Chunming Tang 写的“可分开的离线/在线签名”；PKC 2009：Dan Boneh, David Freeman, Jonathan Katz, and Brent Waters 写的“签名一个线性子空间：对网络编码的签名体制”；Ivan Damg˚ard and Gert L Mikkelsen 写的“个人数字签名的理论和实践”；Marc Fischlin and Dominique Schr¨oder 写的“在终止条件下的盲签名安全”； Christina Brzuska, Marc Fischlin, Tobias Freudenreich， Anja Lehmann, Marcus Page, Jakob Schelbert， Dominique Schr¨oder, and Florian Volk 写的“重新认识 Sanitizable 签名的安全”；Brian J. Matt 写的“基于对子群签名的多方无效证明”；Toru Nakanishi, Hiroki Fujii, Yuta Hira, and Nobuo Funabiki 写的“恢复群签名体制对签名和认证的固定消耗”；Jan Camenisch, Markulf Kohlweiss, and Claudio Soriente 写的“基于双射的累加器和对匿名资格的有效恢复”；Scott Coull, Matthew Green, and Susan Hohenberger 写的“使用固定匿名资格的健忘数据库的控制接入”。

九、多方协议

RSA2009 会议：Tomas Toft 写的“秘密共享值的固定圈、几乎线性比特分解”；Andrew Y. Lindell 写的“对同时构造的本地顺序没有帮助”； *Ignacio Cascudo, Hao Chen, Ronald Cramer, and Chaoping Xing* 的文章“在任意固定有限域上的强多方共享异步好想法的线性秘

密共享”；第 29 届美密会：*Arpita Patra, Ashish Choudhary, Tal Rabin, and Pandu Rangan* 的文章“可变化的秘密共享重访圈复杂度”；*Juan Garay, Daniel Wichs, and Hong-Sheng Zhou* 的文章“某种程度上的非承诺加密和有效适应健忘传输”；*Joel Alwen, Jonathan Katz, Yehuda Lindell, Giuseppe Persiano, abhi shelat, and Ivan Visconti* 的文章“在调解模型下的随意共谋多方计算”。**2009 亚密会**多方计算（组织：Masayuki Abe）Benny Pinkas, Thomas Schneider, Nigel P. Smart, Stephen C. Williams 写的“实际安全两方计算”；Seung Geol Choi, Ariel Elbaz, Tal Malkin, Moti Yung 写的安全多方计算最小在线边界；Seung Geol Choi, Dana Dachman-Soled, Tal Malkin, Hoeteck Wee 写的使用适时安全协议应用提高非承诺加密；密码协议（组织：Jens Groth）Zongyang Zhang, Zhenfu Cao, Ning Ding, Rong Ma 写的从任意单向函数抽象不可扩展统计隐藏承诺；Giuseppe Ateniese, Seny Kamara, Jonathan Katz 写的从分级身份认证协议抽象的存储证明；Kaoru Kurosawa, Ryo Nojima 写的没有随机预言机制的简单适时键忘传输。

十、理论

PKC 2009：包括数论文章：Alexander May and Maike Ritzenhofen 写的“完全因式分解：仅仅已知一个无致疑的暗示的多项式时间”；Paz Morillo and Carla R`afols 写的“使用列表解密的所有比特安全”；Yoshinori Aono 写的“对 RSA 的部分密钥恢复的格构造”；Minkyu Kim, Jung Hee Cheon, and Jin Hong 写的“对在 F_p^m 域上的 Pollard rho 方法的限制子集随机方法”。**2009 亚密会**（组织：Phong Nguyen）Vadim Lyubashevsky 写的终止 Fiat-Shamir：应用格和基于因子分解的签名；Damien Stehle, Ron Stinfeld, Keisuke Tanaka, Keita Xagawa 写的基于理想格的有效公钥加密；Jonathan Katz, Vinod Vaikuntanathan 写的平滑投射单向函数和从格理论产生的基于口令认证的密钥交换。

十一、其他

Euro2009会议现场张贴目录有两篇来自中国的文章：Xiaorui Sun 和 Xuejia Lai 写的“分组密码算法的密钥独立攻击”。Tao Xie, Dengguo Feng and Fanbao Liu 写的“1-MSB 的差分输入是否会对 MD5 造成快速攻击”。Frederik Armknecht, Ahmad-Reza Sadeghi, Pim Tuyls, Roel Maes and Berk Sunar 写的“物理不可克隆伪随机函数”。Endre Bangerter, Jan Camenisch, Stephan Krenn, Ahmad-Reza Sadeghi and Thomas Schneider 写的“合理零知识协议的自动生成”。C′eline Blondeau and Benoˆıt G′erard 写的“抗分组密码算法的统计攻击的数据复杂性”。Dan Boneh and L′eo Ducas 写的“从非对称到匿名：对匿名 HIBE 的新构造”。Emanuele Cesena 写的“重新访问超单零迹的配对变化”。 Ming-Shing Chen, Jintai Ding, Chia-Hsin Owen Chen, Fabian Werner and Bo-Yin Yang 写的“隐藏域等式的奇变量多重变换”。 Rafa¨el Fourquet, Pierre Loidreau and C′edric Tavernier 写的“查找分组密码算法好的线性逼近和对减轮 DES 的分析应用”。 Owen Harrison and John Waldron 写的“图论过程里的加速公钥算法技术”。 Miia Hermelin, Joo Yeon Cho and Kaisa Nyberg 写的“使用 Matsui’s 算法1的多方位扩展的密钥恢复统计测试”。 Paulo Mateus 和 Serge Vaudenay 写的“在可信代理模式下的隐私丢失”。Karsten Nohl and Mate Soos 写的“使用最优化SAT解决低复杂度密码体制”。Tatsuaki Okamoto and Katsuyuki Takashima 写的“一个在配对和分别登记断言加密里的几何方法”。Jacques Patarin and Joana Treger 写的“对FEISTEL 网络进行内部置换的一般攻击”。Kun Peng and Bao Feng 写的“通过一个蒙特函数泄露的一个离散对数测试范围正式讨论”。

Euro2009：特邀讲话：Shafi Goldwasser 的“没有（几乎没有）任何秘密的加密体制”。FSE2009 会议收录的文章：中国文章两篇：使用低代数阶的分组密码新的分析理论——Bing Sun, Longjiang Qu and Chao Li，国防科技大学, 中国东南大学；使用秘密前缀方法的对 MAC 的新的区分攻击——Xiaoyun Wang, Wei Wang, Keting Jia, and Meiqin Wang，清华大学，信息安全国家重点试验室。RSA2009 会议：Rafael Dowsley, J¨orn M¨uller-Quade, and Anderson C.A. Nascimento 写的“在标准模型下基于 McEliece 假设的公钥加密体制 CCA2 安全”；Crystal Clough, John Baena, Jintai Ding, Bo-Yin Yang, and Ming-shing Chen 写的“SQUARE：一个新的多变量加密体制”；Matthew Franklin, Mark Gondree, and Payman Mohassel 写的“对最长共同序列的有效通信秘密协议”；Giuseppe Ateniese, Karyn Benson, and Susan Hohenberger 写的“秘密密钥范式重新加密”；Man Ho Au, Patrick P. Tsang, Willy Susilo, and Yi Mu 写的“对 DDH 群的动态广泛聚积和他们在基于属性的匿名认证体制的应用”；Anna Lisa Ferrara, Matthew Green, Susan Hohenberger, and Michael tergaard Pedersen 写的“组证明的实践短签名”； Dae Hyun Yum, Jae Woo Seo, Sungwook Eom, and Pil Joong Lee 写的“用几乎完美复杂度的单层片段 HASH 链变化”；Masayuki Yoshino, Katsuyuki Okeya, and Camille Vuillaume 写的“对他们的商没有抽取消耗的递归双模乘法”；PKC 2009：Dan Boneh, David Freeman, Jonathan Katz, and Brent Waters 写的“签名一个线形子空间：对网络编码的签名体制”；Pascal Junod, Alexandre Karlov, and Arjen K. Lenstra 写的“提高 Boneh- Franklin 反叛追踪体制”；M. Choudary Gorantla, Colin Boyd, and Juan Manuel Gonz′alez Nieto 写的“基于组密钥加密模型构造密钥折中假冒模型攻击”；Aggelos Kiayias and Hong-Sheng Zhou 写的“使用删除证据的零知识证明”；第 29 届美密会：*Marc Stevens, Alexander Sotirov, Jacob Appelbaum, Arjen Lenstra, David Molnar, Dag Arne Osvik, and Benne de Weger* 的文章“对 MD5 的选择谓词短碰撞攻击和一个 ROGUE CA 证书的产生”；*Kazumaro Aoki and Yu Sasaki* 的文章“减轮 SHA0，SHA1 的中间人范式攻击”；*Edward W. Felten* 的文章“ALICE 和 BOB 到华盛顿：一个权术和策略的密码理论”；*Stanislaw Jarecki and Xiaomin Liu* 的文章“秘密相互认证和条件健忘传输”；*Mira Belenkiy, Jan Camenisch, Melissa Chase, Markulf Kohlweiss, Anna Lysyanskaya, and Hovav Shacham* 的文章“随机化证明和可代表的匿名证书”；*Ilya Mironov, Omkant Pandey, Omer Reingold, and Salil Vadhan* 的文章“可计算得差分秘密”；*Yael Tauman Kalai and Ran Raz* 的文章“概率可查证论据”；*Rafael Pas, Wei-Lung Dustin Tseng, Douglas Wikstr\"om* 的文章“公共硬币的零知识协议的构造”；*Ronald Cramer and Ivan Damg{\aa}rd* 的文章“零知识协议的分摊复杂度”；*Jens Groth* 的文章“子线型零知识争论的线性代数”；*Brent Waters* 的文章“双系统加密：认识足够安全的 IBE 和在简单假设下的 HIBE”；*Dennis Hofheinz and Eike Kiltz* 的文章“二次剩余签名和应用的群”；*Susan Hohenberger and Brent Waters* 的文章“从 RSA 假设出发的短和固定签名”；*Michel Abdalla, C\'{e}line Chevalier, and David Pointcheval* 的文章“为条件承诺获取的平滑映射单向函数”。 CHES2009：Ghaith Hammouri, Worcester Polytechnic Institute, USA， Aykutlu Dana, Bilkent University, Turkey，Berk Sunar, Worcester Polytechnic Institute, USA 写的“CDs 也有指纹”；Francesco Regazzoni, UCL, Belgium and ALaRI, Switzerland，Alessandro Cevrero, EPFL, Switzerland，François-Xavier Standaert, UCL, Belgium，Stephane Badel, EPFL, Switzerland，Theo Kluter, EPFL, Switzerland，Philip Brisk, EPFL, Switzerland，Yusuf Leblebici, EPFL, Switzerland，Paolo Ienne, EPFL, Switzerland 写的“对抗 DPA 指令集扩展的一个设计流和评估框架”。

2009 亚密会特别报告：IACR 特别报告（IACR 主席：Bart Preneel）Tatsuaki Okamoto 的一个双向配对的新方法和它的应用。

十二、黑帽大会

2009 美国黑帽大会于 7 月 25 日—30 日在拉斯维加斯举行。主要内容包括：ALE SSANDRO ACQUIS TI 写的“作者发现 1 亿 SSN”：作者可以已知的个人的地理位置和生日进行预测社会保险号码（SSN）；DMI TRI ALP EROVI TCH, K EI TH MUL ARSK I 写的“从技术层面 打击俄罗斯网络犯罪”：从 FBI 和俄罗斯本土安全研究进行的特别监听代理，在过去十年，以他们的经验加强抗俄罗斯和基于欧洲财团的在线犯罪最著名案子的深度报道。ANDRE A B ARISANI , DANIE LE B IANCO 写的“在线使用能量和电力泄漏的光样本对激光、电压键盘敲击嗅探边信道攻击”：模版攻击、探索电磁排放搜集数据，经常通过安全通信和成为门类（作者猜测为 NSA 雇员）；ROD BECK STROM 写的“Be c k s t r om's 定律：对价值网络安全的模型”：是一个粒度和转换作用可以在任何价值网上进行使用；MARC B EV AND 写的“在 GPUS 上选择前缀 MD5 碰撞攻击”：2008 年 12 月，一个选择前缀的 MD5 碰撞攻击，在一个 3 簇的工作产生一个 CA；BI L L BLUNDEN 写的“抗预测：Ro o t k i t 连接”：连接 Ro o t k i t 主要研究突发回应打击和使用一种变化的承诺策略进行监听；HRIS TO BOJ INOV, DAN BONEH, EL IE BURSZ TEIN 写的“嵌入管理界面：融合 MA 不安全：在最近几年，设备的数量从网络激烈的增加对嵌入友好管理界面访问。从轻型管理系统到 SOHO NAS 应用到像片框架，在所有的设备可以发现这些界面。” MICHAE L BROOKS , DAVID A SLANIAN 写的“Bi t To r re n t 黑客”：这是两个海盗攻击 Bi t To r re n t 的过程，滥用 Bi t To r re n t 协议的表面途径，发现 Bi t To r re n t 客户的协议，找到 Bi t To r re n t 客户和开发，同时将测量这些攻击；JE SS E BURNS 写的“探索轶事诊断”：在综合编程环境和一个特殊的安全模型下，基于 LINUX 的电话系统是难于被拒绝开机的。一个应用层的独立，对通常新核心简单数，假设包括公开来源热度的 UI 特征将开发 A n d r o i d 的猜测新核和用户模型机制，怎样测试，怎样在 DROID 环境下进行混合；K. CHEN 写的“修复和开发 APPLE 一个固定件升级”：描述一个攻击者在 APPLE 铝制键盘上能够安全恶意代码；MA T T CONOVER 写的“SADE：注入代理到客户 OS 的 VM”：当虚拟（VM）机越来越多的被包括到物理层，反应到在相同的物理层可以显著的减少运行资源消耗，有 VM 共享内核元件。DINO DA I ZOVI 写的“高级 MAC OS X Ro o t k i ts”：因为 MAC OS X 是一个特殊的 BSD 和前进内核，当面向 UNIX 的 Ro o t k i ts 技术广泛公开，基于 MACH 的 Ro o t k i ts 技术已经被广泛的探究。报告将包括一个对用户空间到核心空间 Ro o t k i ts 技术并且内核空间 Ro o t k i ts 唯一使用，并且低级的估计文件 MAC Ro o t k i ts OS 系统和 MACH 特征；“亚稳态的污点”：比给一个 Remo 外壳有更多的一系列几年的 MAC 开发。DA TAGRAM 写的“亚稳态的锁检”：锁检被描述为最后进入方法，不可探测和瞬间发生，只要关心拍摄。更进一步的事实是没事，这个话题的免费可用的信息几乎无法查找。这个话题将聚焦在小范围和顺便带到的几种形式的证据片断；MIKE DAVIS 写的“可恢复的高级 METERING 结构”：智能网格、智能仪表，AMI，当然没有人可以逃离，但是潜在的基础破坏技术包围。然而，平等的产生嗡嗡声强调这些攻击技术。NITE SH DHANJANI 写的“Ps y c h o t r o n i c a ：探索、控制和欺骗”：从新的通信模式揭示公共信息的脆弱，例如社会网络的应用可以使你远程俘获关于个人目标的私密信息；MARK DOWD, RYAN SMITH, DAVID DEWEY 写的“信任的语言：在活动含量里揭示可信关系”：一起活动的含量称为增加的权利和最近几年更灵活的方法，使用主要的函数附加在基于网页的技术，例如 JAVA 脚本，.NET 和通过插件浏览。MUHAIMIN DZUL FAK AR 写的“高级 MYSQL 探索”：这个发言集中在M Y S Q L 和S Q L 注入弱点能够在L A M P 和W A M P 环境使用远程代码执行；MICHAE L EDDINGTON 写的“秘密模糊”：模糊时生命周期安全发展的重要部分

（SD）和攻击防御安全研究者、顾问甚至是软件开发者一个普通工具；EGY PT 写的“在顺便开发里使用可制导导弹：自动浏览指纹和亚稳态的开发”：黑帽社区已使用了客户一边的开发了几年；RACHEL ENGEL 写的“Gizmo：一个轻型开放网络代理”：Gizmo 是一个面向轻型速度和分别的免费开放源头网络代理。当一些人执行一个网络测试，他们希望有一个工具进行编辑和通过快速请求进行搜索；STEFAN E SSER 写的“在稳定 PHP 环境下后开发状态”：当一个攻击者试图执行在网络应用绝对的 PHP 代码，现在经常在 PHP 环境下不仅仅对安全模式，基础含量和可使用函数的 PHP 使用相互保护，也包括 S u h o s i n 的使用和操作系统，文件系统和数据库水平的安全机制，例如：A S L R, NX ,硬件内存管理和 UNIX 文件许可；TONY F L ICK 写的“黑客和智能网格”：MIAMI 市和几个商业伙伴计划到 2011 年开发了“覆盖城市的电力智能网格”，在这个谈话里作者主要讲解目前指南和路线图的缺陷和几个关键的控制点，包括支付卡的关键工业安全标准（PCI DSS），整个系统过度依赖组织；ANDREW FRIED, P AUL V IXIE, DR. CHRIS LE E 写的“互联网特殊 OPS：通过数据挖掘大幅度进展”：作者将提出数据挖掘的简介，提出几种使用身份的快速连续改变和怎样使用相同的信息进行列举和叙述；CHRIS GATES 写的“使用亚稳态进行破解和不可破解的预言机制”：作者给出了一个预言机制的表出方式，并且对亚稳态附件进行了不可破解的预言进行了破解；TRAVIS GOODS PEED 写的“一个 16 比特 Ro o t k i t 和第二代 Zigbee 芯片”：对无线传感网络提供 Ro o t k i t 的自我复制，对第二代 Zigbee 无线电芯片，例如 EM250 的 CC 2 4 3 0 / 2 4 3 1。这篇文章同时给出一个生动的演示和弱点；JOE GRAND, JACOB A PPELB AUM, CHRIS TARNOVSKY 写的“智能停车，全球化和 Y”：作者对电子停车的评估和智能卡协议分析竞争，硅淘汰分析，固定件恢复机制，在成功的分枝；JENNIFER GRANICK 写的“计算机犯罪年评介：我的空间，MBTA，BOSTON 大学”：作者从网络犯罪案件里分析一些原因，对计算机最新安全法规的进展进行合法研究的挑战；JEREMIAH GROSSMAN, TREY FORD 写的“钱越多问题越多：使用更多的黑帽方法进行网络运做”；PETER GUERRA 写的“经济和信息安全怎样影响网络犯罪和全球经济衰退意味着什么”；NA THAN HAMIEL , SHAWN MOYER 写的“网络武器：对产生用户含量的更进一步攻击”：最后，在用户产生的站点的建议，是在俄罗斯轮盘的一种变量，每轮枪会指到你的头部，无论参与者的数量。你可以赢得更多的时间，但是最后一颗带有你名字的子弹会找到自己的线路；NICK HARBOUR 写的“翻转获胜：通过在线垂钓跟踪和沙盒计算”：这个谈话将讨论一个新的翻转机制的免费工具 API 窃贼，“我赢得”了 MAL 中间件分析的按钮。唯一的办法是工具操作必须开发，只要能够提供更好品质，比目前使用的追踪工具更先进；RILEY HA SSELL 写的“探测丰富含量”：作为 RIA（丰富互联应用）技术带动市场许多疑惑，影响安全前景的压力；CORMAC HERLE Y, DINE I F LORENCIO 写的“经济学和背景经济”：网络犯罪目前是非常大的部分，额外的时间导致直接的经济损失，例如，一个没有水平的垂钓者产生直接的经济损害，甚至没有经济增长；BILLY HOFFMAN, MAT T WOOD 写的“发行：基于浏览的黑网”：黑网的概念是近几年流行的，指对匿名通信的用户在安全通信和共享文件时隐藏网络背景。这篇文章讨论和证明揭示概念证明和基于浏览的黑网；MIK KO HY PPONEN 写的“神秘的 Conficker”：假设网络蠕虫已经死了，现在证明其仍然存在。这篇文章呈现的是作者对 Conficker 的分析，揭示了网络过滤使用的机制和产生域的算法；VINCENZO IOZZO, CHARLIE MILLER 写的“探索后幸运：一个 IPHON 制造厂的 Me t e r p r e t e r 装载”：文章给出了怎样在高级别的装载过程里，IPHON 工厂通过缺省代码签名进行开发安全保护；DAN KAMINSKY：“关于网络安全的一些情况”；MIK E KERSHAW 写的“Kismet 和 MSF”：演示客户可以对 TCP 流污染抗普通的网站攻击，装载 MSF 到客户，修改已经发送的 TCP 流的结尾；PETER K LE IS SNER 写的“St o n e d Bo o t k i t”；KOS TYA KORTCHINS KY 写的“云爆炸：3D 黑客”：云爆炸是 VMware、MACOS 和

MALWARE 在三种虚拟视频文件合成的，允许用户在主机上执行代码；ZANE LACKEY , LUIS MIRAS 写的“SMS 攻击”：通过敌意的 SMS 拥塞发现目前的移动设备的音频威胁；AARON L EMAS TERS, MICHAEL MURPHY 写的“快速企业测试：怎样运行一个折衷网络，保证数据安全”：作者使用的快速方法对大量的突发事件反应过程。与只针对个人用户和主机的部分网络片断不同，作者采用的方法特征是隔离网络包括的威胁和保持可运行的核心商业函数；FELIX " FX " L INDNER 写的“路由探测”：积极网络设备的探测有自己的历史和挑战。对可能的攻击全频谱会话，在最近的特殊范围进行探测。在 CISCO 设备环境下对表面进行攻击，对其他的范围的种类进行对比；JOHNNY LONG 写的“我到我们”；KEVIN MAHA FFEY, ANTHONY L INEB ERRY, JOHN HERING 写的“你的移动电话是否安全：对移动通信的视频攻击和防护”；MOXIE MARL INSPIK E 写的“对过失 SSL 的更多欺骗”：这篇文章给出一些新工具的刻画，对这些通信点进行欺骗，最终提供对 SSL/TLS 的高效攻击；JOHN MCDONA LD, CHRIS VALASEK 写的“WINDOWS 2003/XP 里的实践堆积探测”：这篇文章是对基础的发展和实践堆积的进一步研究；HAROON MEER, NICK ARVANI T IS, MARCO SLA VIERO 写的“云追踪”：S e n s e P o s t 在这篇文章里对“云”的几种云的攻击和使用这些工具产生互联网混乱；EREZ METULA 写的“管理代码 Ro o t k i ts：运算环境钓鱼”：这个谈话将介绍“.NET-SPLOIT”的新版本，一个修改语言的普通工具，用来完成 Ro o t k i ts 概念，这篇文章提供原代码；CHARL IE MI L L ER, COL L IN MUL L INER 写的“在你的电话里进行电话混乱”：这篇文章里找出智能电话的弱点；CHARL IE MI L L ER, COL L IN MUL L INER 写的“死的网屏：对废弃网屏应用产生一个特洛伊屏幕系统的进展”：这篇文章细致的描述了废弃网屏平台可以通过安装攻击调整固定件进行完全的转化，固定件是一个有效的嵌入 Ro o t k i ts；STEV E OCEP EK 写的“长期会话：为什么我们不能有好的事情？”：这篇文章讨论了长期会话的分类，决定使用方法和连接和不连接的方法；JEONGWOOK OH 写的“抗打击一天探测：不同的二进制和抗不同的二进制”：安全补丁的使用意味着固定安全的脆弱；AL FREDO ORTEGA , ANIBA L SACCO 写的“探测 Ro o t k i ts”：应该有三种事情产生 Ro o t k i ts（1）如果你有笔记本，你也许有 Ro o t k i ts（2）如果你无法去掉 Ro o t k i ts，那么你也许可以知道怎样探测（3）最后，你也许知道怎样可以激获 Ro o t k i ts； THOMA S H. PTACE K, DAV ID GOLDSMI TH, JEREMY RAUCH 写的“黑客资本‘09：市场的脆弱和交易资本”：通过系统和协议使用指导这个商业运行，一个并行的互联网是金钱路由和 PORN，MP3 的合同；DANNY QUIST , LORIE L IE BROCK 写的是“Cr a y o n 机制的恢复：基于 MALWARE 分析和虚拟游戏改变符号”；TI F FANY STRAUCHS RAD, JAMES ARL EN 写的“你的想法：合法状态，权利和自身安全”；DANIEL RA YGOZA 写的“自动 MALWARE 类似分析”：这篇文章是在深度分析的 MALWARE 样本时进行最好的配合，查找进一步连接，减少复制企图；BRUCE SCHNEIER 写的“重新进行安全概念”：当我们拥有了实际的安全时才能感觉和实现安全的范围；PETER SI LBERMAN, STEV E DAV IS 写的“自动间谍中间点：重新构造犯罪现场”；VAL SMITH, COL IN AMES , DAVID KERB 写的“中间钓鱼”：远程攻击使用的方法；ALE XANDER SOT IROV , MIK E ZUSMAN 写的“破解扩展有效 SSL 证书的神秘安全”；KEV IN S TADMEY ER, GARRE TT HELD 写的“好上加好的坏处”：这个谈话提供了通常的概况，已知少量和发现安全相关的脆弱，很少知道奖励范围；ALE X STAMOS, ANDREW B ECHERER, NATHAN WI LCOX 写的“云计算模型和脆弱性：新的炫耀趋势”：作者的目标是探测不同的统计方法，提供云计算安全模式的比较，设计出安全的云计算模型；BRYAN SUL L IV AN 写的“防御重写：对 XSS/XSRF/重新路径的钓鱼防御”；CHRIS TARNOVSK Y 写的“内部的黑暗是怎样的？”：最新的 128 算法是否安全，是否存在智能卡的读取方法；ALE XANDER TERESHK IN, RAFA L WOJ TCZUK 写的“包括 3 环的 Ro o t k i ts”；STEV E TOPL ET Z ,

JONATHAN LOGAN AND KY LE WI L L IAMS 写的“全球间谍网络：在现代信号情报条件下的现实可能性”; MICHAE L TRACY, CHRIS ROHL F , ERIC MONT I 写的“PENTESTERS 的 RUBY”； DUS TIN " I)RUID" TRAMMEL L 写的“亚稳电话”； EDUARDO VE LA NA VA , DA VID L INDSA Y 写的“我们喜欢的 XSS 过滤和怎样攻击”； MARIO VUKS AN, TOMISL AV P ERICIN 写的“快速和疯狂的恢复 TITAN 机制”； CHRIS WE BER 写的“拆开单独代码：对打击虫的计谋袋”； JE F F WI L L IAMS 写的“企业 JAVA Ro o t k i ts”； RA FAL WOJ TCZUK, A LEX ANDER TERE SHKIN 写的“攻击 INTEL BIOS”； PANE L DISCUSS ION 写的“脆弱研究版本规律 2.0：比较关键工业结构”：这篇文章近距离检查 CONFICKS 蠕虫和远程 WINDOWS RPC 反应这种关键的条款和防止在企业的注入。PANE L DISCUSS ION 写的“CSO 小组：黑帽策略供给”； PANE L DISCUSS ION 写的“在媒体里分析安全研究”：政府黑客导致结构的高水平，这篇文章聚焦在安全细节的驱动，是否脆弱的表面和新的攻击是一个好的网，媒体流会被污点快速覆盖；PANE L DISCUSS ION（小组讨论）题目是“DC 小组：从华盛顿升级”； “VC 小组：在会话里的安全业务策略”； “供应关系：供应和超出供应”； “一个黑帽脆弱的冒险评估”； “Pwnie 奖励”； “2009 黑客法庭：在 138 或更少的字符描述经济”。

2009 欧洲黑帽大会于 4 月 14 日——17 日在阿姆斯特丹举行，主要发言人和话题包括：Chema Alonso 和 Enrique Rando：使用中间数据的策略指纹，隐藏信息和丢失数据；Craig Balding：一个云安全的核心报道；Emmanuel Bouillon：驯服野兽，评估 KERBEROS 保护协议； Benjamin Caillat： WiShMaster WINDOWS 熟练 SHELL 代码； Bernardo Damele Assumpcao Guimaraes：对完全控制的操作系统进行高级 SQL 注入探测；Eric Filiol：公开办公系统的设计弱点；Hagen Fritsch：今天书柜里的新书：在 LINUX-x86-64 的缓存溢出保护的现状；Roberto Gassira' and Roberto Piccirillo：移动数据连接攻击；Rob Havelt：尽管非常高保真，但不是没有内在安全；Anthony Lineberry：在用户地域上的 ALICE：通过 DEV/MEM 攻击 LINUX 内核；Bruno Luiz：转换状态：对正式核查进行基于竞争的安全测试；Moxie Marlinspike：在实际应用里把 SSL 模版转换为缺省 HTTPS；Moxie Marlinspike：.NET 构架 Rootkits，在你的结构内部的后门；Charlie Miller and Vincenzo Iozzo：MAC OS X 和 IPHONE 支付游戏和乐趣；Jon Miller, Alex Wheeler, David Bonvillian, and Neel Mehta：从大量宣传里切入，应用测试方法论的分析；Mariano Nunez Di Croce：SAP 渗透测试；Mariano Nunez Di Croce：轮换，面向 INTERNET 的 SAP 服务测试，SAP 路由；Enno Rey and Daniel Mende：你钱包里所有归我们，攻击骨干技术；Rich Smith：VAASeline，VNS 自动服从攻击；Roelof Temmingh and Chris Bohme：使用开放资源工具的防守和攻击粘合 Maltego；Jeroen van Beek：可移动的护照签署；Chris Wysopal：探测“预先拥有的证书”软件和设备；Stefano Zanero & Claudio Criscione：Masibty，基于异常探测的网络应用防火墙。

十三、结论

2009 年的国际密码年会与 NIST 的 SHA3 活动进行了衔接，因此在文章里有所表现。整个密码学界仍然是按照密码学的几个大的分支在进行越来越深入的研究，获得一些细致的结论。从 SHA3 的算法 Keccak_Round2 已可以看出一些密码学与智能处理、活动环境选择之间交叉融合，另外也有算法在输入、输出方面进行了一些自动化的尝试。只是，随密码使用的逐步扩展，特别是在开放网络的使用，由于环境的不确定和变化，密码体制里的机器或自动学习机制也是值得应用研究关注的一个方面。

参考文献：

WWW.IACR.ORG，2009