一、SHA-1 碰撞攻击的改进

2004 年王小云提出了比特追踪法，可以给出 SHA-0、MD5、RIPEMD 和 MD4 的有效碰撞攻击。但是 SHA-1 比 SHA-0 具有更强的雪崩效应，SHA-1 的分析存在很多理论难点，其中不可能差分是破解 SHA 系列的理论障碍。因此王小云提出将不可能差分路线转化成概率为 1 的差分路线思想，找到了 SHA-1 的碰撞路线。但是推出的 SHA-1 碰撞路线的前提条件中有 70 多个条件是含有 512 个变量的明文比特线性方程，构成实施明文修改提高碰撞概率的障碍。为了修改一个错误比特条件，需要对明文进行修改，但一个明文比特的改变将破坏约一半的明文比特方程。故提出系统的明文修改技术与控制方法，既保证明文比特方程成立，又纠正差分路线中出现的不成立的比特条件，给出了 SHA-1 的有效攻击，攻击效率为 2^{63} 次运算，该结果作为 keynote speech 在 2005 年 11 月 NIST 举办的国际 Hash 函数研讨会上公布。2006 年 1 月将破解效率提高到 2^{61}，该结果在 2006 年 RSA 大会上作为特邀报告。

《SCIENCE》评论“SHA-1 的攻击足以引起密码学家的担忧”。针对 SHA-1 的改进结果，NIST 宣布“NIST 承认王确实发现了 SHA-1 的实际碰撞攻击”。

NIST 宣布“美国联邦机构在 2010 年前必须停止 SHA-1 在电子签名等基于无碰撞特性的密码应用”，并启动了国际 Hash 函数新标准 SHA-3 的五年设计工程。

二、SM3 密码杂凑算法

2005 年 3 月，针对实验室主任王小云教授采用自主研发的比特追踪法破解 MD5 等算法的情况，国家密码管理局高度重视，组织专家组对我国已有的 Hash 函数算法进行了针对性分析，并下达紧急任务设计一个安全高效具有我国自主知识产权的 Hash 函数算法。在此基础上，以王小云教授为首的专家组运用最先进的杂凑算法分析和设计理论研制了 SM3 算法。该算法采用了新颖的消息扩展算法、双字介入的并行压缩结构以及混合使用不同群运算，有利于消息的扩散和混乱，便于软、硬件实现。

SM3 经过国家密码管理局组织专家评估，没有发现超过算法一半（32 步）的理论攻击，特别是没有发现超过 9 步概率有效的碰撞路线。而国际设计的 Hash 算法则存在 1 圈（16-20 步）的概率为 1 的碰撞路线。SM3 算法的设计适

合于软硬件实现，软硬件评估结果总体优于 SHA-2（NIST 设计的 SHA-1 备用算法），经专家评估整体设计水平国际前列。

SM3 算法由国家密码管理局 2010 年正式发布，是我国公开的首个实用化 Hash 函数算法，已在政府、军工、金融及企业等重要社会与经济领域推广使用。该成果获得 2009 年国家发明专利，并获 2010 年国家密码科技进步一等奖（省部级）。在国家密码管理政策的支持下，通过推行 SM3 等密码算法，一批民族企业研发了大量商用密码产品，带动了民族产业的发展，增加了就业岗位，客观上加强了密码在信息安全中的支撑地位。

三、MAC 算法的新分析方法

随着国际通用 Hash 函数 MD5、SHA-1 等算法碰撞攻击的提出，基于 Hash 函数的 MAC 码的安全性引起国际密码社会广泛的关注。2005 年，王小云提出了基于 MD4 碰撞路线的密钥前缀 MAC 的分析方法。随后基于王小云、于红波等 MD4 的高概率碰撞路线，国际密码学家给出了基于 MD4 的 HMAC/NMAC 算法的安全性分析。但是大多数 Hash 函数的碰撞路线有太多的条件，似乎不能用于 MAC 的分析。国际上通用的是 Preneel 的生日攻击方法，通过识别内部碰撞进行伪造攻击，但是该方法是一个通用的攻击，并不能识别算法，也不能进行密钥恢复攻击。

2008-2009 年针对一系列 MAC 算法，我们提出了基于生日攻击分析的新思想，即区分带差分路线的内部几乎碰撞或碰撞新方法，给出多种重要 MAC 算法的理论攻击结果，打破了只能通过识别不带差分路线的碰撞进行安全性分析的常规思路，为多种 MAC 算法的安全性分析带来新思路。具体安全性分析结果如下：

（1） HMAC/NMAC 的安全性分析

HMAC/NMAC 是 1996 年 Bellare 提出的基于 Hash 函数的 MAC 算法，HMAC 是 NIST 标准。首次给出不利用相关密钥的 HMAC/NMAC-MD5 的区分攻击，并将该攻击用于 MD5-MAC（ISO 标准）的部分密钥恢复攻击，为 MAC 算法的安全性分析带来新思路。论文发表在国际会议 Eurocrypt 2009。

（2）以分组密码和缩减轮数的分组密码为主要部件的 MAC 算法的伪造攻击

给出了 Alred 结构，Alpha-MAC，PELICAN，MT-MAC-AES 和 PC-MAC-AES 的区分攻击，等价密钥恢复攻击和密钥恢复攻击，论文发表于国际会议 Crypto 2009。其中 Alred 结构，Alpha-MAC 和 PELICAN 是由 AES 的设计者 Daemen 和 Rijmen 提出的。

该方法也适用于分析其他的一些 MAC 算法，如基于 Haval 算法的 HMAC/NMAC，基于约减轮数的 SHA-1 和 SHA-2 的 LPMAC 和 CBC-MAC 等。

四、分组密码与序列密码的安全性分析

对国际上通用的重要分组密码算法和序列密码进行安全性分析，不仅采用经典的差分、线性分析方法还探讨一些新的安全性分析方法如 Linear Hull，三明治（Sandwich）攻击等。

(1) 分组密码的安全性分析

通过研究环上乘法运算例外点的非随机性，结合差分分析方法，给出分组密码算法 MMB 全算法的理论破解结果，随后又使用三明治攻击，给出了 MMB 算法的实际破解；通过研究 Linear Hull 中相关路径的影响，给出轻量级分组密码算法 PRESENT 的多线性分析，差分分析等分析结果；通过研究非满射大 S 盒的线性和差分特征， 给出了加拿大官方分组密码算法 CAST-128 及进入 AES 第一轮候选算法的 CAST-256 的弱密码假设下的最好分析结果。

(2) 序列密码的安全性分析

成功给出了欧洲流密码工程第二轮两个参赛算法 ABC v3 与 TSC-4 的弱密钥攻击，并淘汰了这两个算法。ABC v3 为欧洲 eSTREAM 工程第二阶段的参赛算法。ABC v3 其密钥长度为 128 比特，该研究通过建立新的数学分析模型，成功给出了该算法的弱密钥攻击，弱密钥个数约 $2^{103.7}$。该研究成果在第二阶段的总结报告中，入选 11 个重要结果之一，第二阶段的评估论文约一百五十篇。算法设计者俄罗斯教授主动与我们联系讨论算法的改进事宜，该研究早期结果曾作为 CANS 2006 的特邀报告与巴黎高师的特邀报告的内容。TSC-4 是基于 T-函数的具有代表性的流密码参赛算法，自公布以来，没有较好的分析结果，T-函数是 Shamir 提出的一种设计密码算法的具有较好安全属性的函数。TSC-4 其密钥长度为 80 比特，我们找到了 2^{72} 个弱密钥。

五、数论与密码数学问题相关研究

在数论与密码数学问题相关研究方面，系统地研究了自守形式理论及其在数论的应用, 拓宽了将自守形式和自守 L-函数应用于数论研究的途径。提出了解决格中最短向量问题的快速算法。对最著名密码体制之一 RSA 密码体制弱密钥问题进行了深入研究。

（1）自守形式理论在数论中的应用

Lindelof 猜想是自守 L-函数理论的三大猜想之一。证明了一类阶为 4 的 Rankin-Selberg L-函数的 Lindelof 猜想在平均意义下成立, 推出了这类函数的亚凸性上界。进而证明了 Sarnak 的 QUE 均匀分布猜想。利用自守形式的高等理论, 改进了上述亚凸性上界, 突破 Lindelof 猜想方向上的在凸性界之后的第二屏障。解决了影响深远的 Sarnak 猜想中的若干重要问题。综合应用自守表示的 Jacquet-Langlands 理论、谱理论、二次型代数理论、加权筛法等, 对三元二次型证明了 Sarnak 猜想对殆素数成立，Sarnak 猜想对变量个数大于等于 10 的一类二次型成立。对自守形式等当代先进数学工具用于素数分布的研究探索了新的途径。

（2）求解格中最短向量的快速算法

对格中最经典困难问题最短向量问题，提出两层筛法代替一层筛法平衡时间和空间复杂度，改进了 Phong Nguyen 等提出的目前最好的求解格中最短向量问题的启发式筛法，复杂度通过计算不规则球帽覆盖问题进行估计。论文为 ASIACCS 2011 的特邀报告。

（3）RSA 密码体制的弱密钥攻击

利用连分数方法改进了 2006 年 May 等对基于 CRT 快速实现的 RSA 弱密钥攻击。对满足$|\rho q-p|=N1/4+\gamma$（ρ 已知，$1<\rho<2$，$0<\gamma<1/4$）的 RSA 模，给出了 Fermat 算法时间复杂性的平方根算法分解 N。证明了 LSBS-RSA 密码体制中弱密钥的个数，指出当两个素数 p 和 q 共享$(1/4)^{\log_2 N}$低位比特时该密码体制不安全。