DOI:10.16262/j.cnki.1000-8217.2003.02.004

·学科进展与展望·

信息安全理论与技术的几个进展情况

王育民

(西安电子科技大学 ISN 国家重点实验室,西安 710071)

[摘 要] 本文对信息安全领域中一些问题的进展做点介绍,并谈点个人的看法。包括如下几个问题:(1)量子密码;(2)混沌密码;(3)802.11b WLAN 的发展;(4)进化论与信息安全技术;(5)指纹识别与身份认证;(6)信息安全技术人才培养。所谈意见未必正确,希望得到指正。

[关键词] 密码学,信息安全技术,人才培养

1 量子密码

20 世纪 70 年代初,哥伦比亚大学 S. Wiesner 提出了共轭编码,并指出原则上用它可以用来制造防伪钞票,或将两条消息组合通过单量子传递,在收端可以分路而不相互干扰。但这一有创造性的文章竟被拒刊登,直到 1983 年才得以发表。1979 年 Bennett 和 Brassard 注意到 Wiesner 的观点,可以用来实现保密通信。1989 年,IBM 和美国 Montreal 大学合作,完成了一项令人惊异的实验,在相距 30 cm 的收发两端,以单个光子和精巧的协议,实现了对秘密随机 bit 串的认证。几年后已完成了多项实验。在英国 BT 实验室,利用单光量子和相位编码(Phase Coding),通过 30 km 光纤信道,利用 1.3 mm 半导体激光器,按 BB84 协议安全地进行密钥交换,实现了 20 kb/s 速率的密钥交换,通过改进可望进一步提高速率和传输距离。还有其他类型的量子密钥分配协议,如 Bennett 的二状态协议[1,2],称之为 B92 协议。Hughes 等采用极化编码和更短波长,已经在 14 km 的光纤信道上进行了安全密钥分配的实验;Bennett 等提出一种可以和 BB84 型协议联合或独立使用的协议称之为拒收数据(Rejected data)协议[3];Ekert 根据 Bell 定理提出了另一种基于完全不同物理现象的 EPR 协议,虽然对此已提出实验系统的建议,但尚未实现[4]。BT 实验室还对光纤网中的量子密钥分配技术进行探索,提出了广播树状两级广播中的密钥分配方案[5]。

2001 年 1 月已实现 2 km 距离的自由空间传送[6]。2001 年夏第一个便携量子密码机公开亮相,在晴朗夜空已实现 45 km 的传送。估计在 4—5 年内可以实现将加密的消息通过空间全天候的送到几千里之外,在地面上实现通过轨道卫星传送单光子束,使收发两端可通过卫星实现密钥交换。

根据最近报道[7],量子物理已孕育出市场商品。由 Geneva 大学的几位物理学家在最近几年开始建立的 ID Quantique 公司的第一个新器件是不可破的量子密码密钥协商生成器。2002 年 5 月在德国 Hannover 举办大型消费电子展示会 CeBIT 上,ID Quantigue 的制品激起了观众的极大兴趣。此公司计划在一年内将推出即插即用的量子密码系统,售价约 88 000 美元。如果 Ribordy 成功,这将是一个里程碑,量子信息处理这一新科学的首次商业应用。

虽然这些成果转化为实际应用还要做更多实验研究和产品开发工作,但量子密码的研究成果似乎使人们相信,它可能成为光通信网络中数据保护的有力工具,而且在不太遥远将来,当拥有量子计算能力的密码破译者出现时,量子计算机的计算能力可能足以对付现在普遍采用的各种密码体制,用它来分解大整数、进行离散对数、加解密、搜索密钥等运算的速度将提高许多数量级。那时量子密码可能会提供一种真正安全的密钥分配方式,从而为单钥密码体制提供新的支持。为保护信息安全,量子密码可能是唯一的选择。

实现量子密钥分配的关键技术有二,一是产生

本文于 2003 年 1 月 22 日收到.

单个量子的设备，二是量子检测器。这两种技术都还远未成熟，要实用还需作不懈的努力。

量子密码学所采用的加密方法在几十年前数学上已证明它是不可破的[8]。量子密码理论所提供的绝对安全性在实际实现过程中会存在一些漏洞和不完善之处，攻击者仍会千方百计地加以利用，与攻击者的斗争也将在量子密码新领域中继续进行。量子密码提供了绝对不可破，而不是实际不可破密码。虽然从理论上说量子密码是不可破的，但在实用中仍需考虑安全漏洞。其严重程度尚不清楚，物理学家认为可以用最好的工具堵上大多数漏洞。密码学界的攻击者对此保持有积极的心态。

量子密码所实现的是一次一密体制，这种体制实现了唯密文条件下的不可破译性，但是所付出的代价太大，通常只用于密钥交换。而执行 BB84 协议的代价要比一次一密体制大得多，因此在未来的光量子通信中，它也只能为密钥交换提供一种新的手段，不可能是通用数据加密的方式。利用量子理论实现有效的对数据加密的技术还需做更多的探索，在还没有找到这种加密技术之前，当前的密码算法仍将是数据加密的主流。此外，当前所有量子密码机制在发方和收方之间需要建立在某种普通密码体制的非量子信息交换的认证，用以检测入侵行为。量子密码所用的无条件安全和无条件认证都取自普通密码理论，很难严格区分量子密码和普通密码，我们需要对它们进行适当的组合，来满足信息系统安全的需求。

正如 Western 所说："密码学只有一个，虽然有许多看起来很不相同的密码，但它们的基本思想、目标、和概念总是相同的"。

2　混沌密码

混沌是一种复杂的非线性非平衡动力学过程。

能否驾驭混沌？这是混沌理论研究中的一个重要课题，最近几年的研究表明，有些混沌是可控制、可利用的，而且是十分可贵的。至少在增强激光器辐射功率、调整电子电路输出实现同步、控制化学反应波动、稳定功能异常心脏的心律，以及生成保密通信所需密钥流等方面，可以派上用场。这是基于混沌所具有的以下几个特点。首先，混沌系统的行为是许多有序行为的集合，而每个有序分量在正常条件下，都不起主导作用。但是采用适当方式扰乱一个混沌系统，就可能促使它以其中一个有序行为起主导作用。由于集合中的有序分量足够多且形式多样，因而为应用提供了很大灵活性和机会。其次，混沌看起来似为随机的，但都是确定的。两个几乎一样的、具有适当形态的混沌系统，在同一种相同信号控制或驱动下，即便无人知道其具体过程如何，但它们的输出也是相同的，这是极为有用的性质。最后，混沌系统对初始条件极为敏感，两个几乎相同的混沌系统，若使其处于稍异的初态就会迅速演变成为完全不同的状态。

1989 年 L. M. Pecora 发现，一个混沌系统在满足某种条件下，可以构造成一个同步系统，用此类同步化混沌可以进行通信。同年，Carroll 构造出第一个可同步混沌电路。从此人们开始了将混沌序列用于密码的研究工作。在 *Cryptologia*、*Eurocrypt*、*IEEE on CAS*、*Bifurcation & Chaos* 等杂志和有关会议上发表不少有关混沌密码序列的研究成果[9]。

混沌序列是一种非线性序列，其结构复杂，难以分析和预测，混沌系统可以提供具有良好随机性、相关性和复杂性的拟随机序列，这些都是很有吸引力的特性，使其有可能成为一种可实际被选用的流密码体制。选用何种混沌系统能产生满足密码学中各项要求的混沌序列，是目前各国密码学者大力研究的问题。Matthews 提出用 Logistic 混沌映射经改进成的迭代混沌系统，Carroll 等用 Lorenz 系统，还有 m 序列扰动混沌系统法等。法国 Beaancon 大学 Goedgebuer 等利用可调激光二极管研制了一个光传输数据的系统，它采用混沌叠加加密方式。

国内外的混沌密码研究者对混沌序列抱有很大期望，但是混沌序列用于密码的研究还刚刚开始，有一些重要基本问题尚待解决。首先，混沌序列的生成总是要用有限精度器件实现。这样，任何混沌序列生成器都可归结为有限自动机来描述，在这种条件下是否能超越已有的用有限自动机和布尔逻辑理论所给出的大量研究成果，是一个很值得研究的课题。其次，现有的混沌序列的研究对于所生成序列的周期性、伪随机性、复杂性等的估计不是建立在统计分析上，就是通过实验测试给出的，难以保证其每个实现序列的周期都足够大、复杂性都足够高，因而不能使人放心地采用它来加密。再有，任何特定混沌序列的实现都是由其非线性方程和相应的初始条件完全确定了的，有人在研究跟踪混沌序列进行破译的工作[10]。解决了上述三个问题，混沌序列才可能在密码设计中得到广泛应用。

前面介绍的量子密码和混沌密码都是与物理问题有关的密码，因此有人将密码分为基于数学的密

码和基于非数学的密码。这种提法不够确切,因为密码本质上是数学的,量子理论、混沌理论、乃至宇宙的形成都可以用数学描述。

3 802.11b WLAN 的发展

3.1 有关 802.11 标准[11]

802.11b 标准委员会始建于 1990 年,当时设立了一个任务组负责设计运行在 2.4-GHz 和 5-GHz 频段系统的规范,即现今的 802.11b 和 802.11a 标准。802.11b 和 802.11a 标准于 1997 年推出,是有线 LAN 的扩展,但已成长为一种更有能力、更复杂和令人眼花缭乱的 WLAN。802.11 早期用在少数有无线通信能力的 PC 机,通过单个网络接入点与 Ethernet LAN 连接。由于现实的需求,802.11 委员会已对原标准作了许多扩充,增加了抗干扰、安全、漫游、以及服务质量(QoS)等。

802.11b 可提供 5.5Mb/s 和 11Mb/s 的数据速率。1997 年由美国无线以太网兼容联合会(WECA, Wireless Ethernet Compatibility Alliance)将 802.11b 的商业产品标记为 Wi-Fi。IEEE 802.11a 的数据率为 6 Mb/s—54 Mb/s,美国将 5 - GHz 频段作为无需许可证的国家信息基础设施频段,物理层采用正交频分多路复用(OFDM),与欧洲电信标准学会的 HiperLAN Ⅱ类似。IEEE 802.11g 组的任务是将速度提高到 IEEE 802.11a 水平。IEEE 802.11g 的现行草案采用 802.11a 的 OFDM 的一种变形,以及两种辅助调制方案,即 PBCC 和 CCK-OFDM。使数据率提高到 54 Mb/s。2000 年和 2001 年主要讨论了调制方案。2001 年 12 月出现了突破,今年任务组将要努力完成最后的草案。虽然正式文件要到 2003 年才可能公布,但一些厂商已在准备推出他们的产品。

IEEE 802.11c、d 和 h 是处理特殊的规定和组网等内容。IEEE 802.11e 处理一些对时间敏感的业务,如语音和电视。IEEE 802.11f 涉及支持漫游的接入点的通信。IEEE 802.11i 涉及先进加密标准(AES),支持更强的保密需求。

对 WEP 性能的评价是 WEP 未能达到原定任何一个设计目标。针对密钥流重用的攻击破坏了机密性;针对 CRC 的攻击破坏了消息完整性;针对认证的欺诈破坏了访问控制的安全性;IP 重定向和 TCP 重定向攻击破坏了机密性。同时,WEP 没有定义密钥管理机制,目前 WEP 密钥都是采用手工管理方式的。

从 WEP 失败中可得到一些教训:设计出的标准草案应该面向大众,在接受学术界的普遍分析和检验以后才能被确立为标准;设计安全标准应该有密码学家参与,WEP 的设计者缺乏密码学常识,RC4 本身是一个安全的加密算法,但是 WEP 的设计者没有正确地使用 RC4 算法;设计标准和协议需要汲取以前设计协议的经验教训,误用 CRC 的问题在以前的协议中出现过,但是 WEP 的设计者并没有注意到这一点。

3.2 IEEE 802.11b WLAN 在美国的发展

在美国,无线数据业务已静悄悄地步入快速增长阶段。基于 IEEE 802.11b 的 WLAN 如雨后春笋般地出现,不仅在商业、一些组织内部,而且像等候厅、咖啡馆等公共场所,都大量涌现。现在业务提供商正在将这些"热点"网络串在一起,创建世界范围的无线数据网络。

由于有巨大的发展前景,美国许多大的商家,如 IBM、Intel、AT&T Wireless Services 和 Verizon Communications 在 2002 年 6 月公布,他们可能很快设立一个计划叫做 Rainbow 公司,为商家的出差人士提供 Wi-Fi 业务。Rainbow 公司可能是美国能提供这类业务的最大的计划,最近还有许多新的无线 Internet 提供商,如 Boingo Wireless Inc.、iPass Inc.、Sputnik Inc. 都出售这类业务,使客户能在全国范围利用无线接入点。

3.3 IEEE 802.11b WLAN 在欧洲的发展

欧洲是 GSM 的发源地,也是 3G 蜂窝电话全球标准化组织的领导者,它们最关心的是 IEEE 802.11b 能否嵌入到未来的 3G 标准中去。Wi-Fi 网络的建立和发展与上述问题密切相关。在欧洲到处可以发现 Wi-Fi 也得益于 3G,创造了两者协同的机会,欧洲人所用的各种类型的卡都已客户化,使他们的电话系统最有效地工作。利用无线连接和卡对用户进行认证和收费,并在整个欧洲大陆范围提供安全的 IEEE 802.11 漫游。欧洲大陆的很多公司如:丹麦的 TDC Mobile、瑞典的 Ericsson 和 Telia AB、芬兰的 Nokia 和 Sonera、西班牙的 Telefónica SA 以及比利时、德国、荷兰和英国的一些公司都在积极参与这项技术的开发和运营工作。

3.4 Wi-Fi 与 3G 的关系[12]

Wi-Fi 与 3G 有竞争,但欧洲的发展表明两者有很大互补性,未来的发展可能会进一步证明这点。基于蜂窝的数据业务为用户提供无缝和移动性,WLAN 可提供高数据率。

有些人认为,Wi - Fi 的增长是由于 3G 蜂窝系

统的成本高，开发商用于购入3G频谱的使用权的付出很大。GPRS被看作是到3G的过渡。GPRS在欧洲启动缓慢，3G的引入也比计划迟缓。而基于IEEE 802.11WLAN的技术发展很快，原因一是数据速率，另一个可能更重要的理由是价格，当前通过公共网络传送1 Mb的费用为0.2到0.4欧分之间，而GPRS网络需要3到38欧分。

有人估计，实现IEEE 802.11和GPRS/3G之间的无缝业务估计还要一年的时间。在网际漫游成为商业现实之前，必须解决认证、收费和QoS等技术问题。

4　进化论与信息安全技术

近年来科技界有一个新动向，那就是达尔文进化论思想的复苏。人们想发展一些新的理论来构造一些具有自适应、自组织、自我完善、自我超越和自我进化能力的系统。这种新达尔文理论在许多领域都有体现：如突变、DNA结构、生殖遗传学等。

生物之所以能进化，其核心不是自适应性，而是创造性。蓝绿藻是最具有适应性的生物，其繁殖能力无与伦比，这为几十亿年的生物史所证明，但它不具有创造性，因而也就没什么进化。生物进化之谜将由具有创造性的进化动力学、自我超越动力学或自组织动力学来揭示。

进化思想在IT领域也有表现。例如，MIT计算机科学实验室正在开发的一种全新的信息技术，称为氧系统(Oxygen system)[13,14]。氧系统中包含一个子项目，称作原始芯片项目，它为氧系统开发一种全新的微处理器，具有灵活的设计、空前的传输数据的能力、能量效率和成本效益，为软件提供所需的运行环境。

“原始芯片”由许多完全相同的矩形块组成，每个矩形块都有内存单元和功能单元，并有一个开关控制连接相邻两个矩形块的线路。芯片内部采用多路复用器编程法提高矩形块之间的连接效率。编译器通过对芯片进行线路编程所形成的“软线路”可精确调动信号，使其沿最佳路径传送。它的传送和处理数据的能力和速度都将大大高于现有芯片。到2010年它的钟频可达10—15 GHz。MIT业已研制出10倍于当前处理器的“原始芯片”。目前正在研制开发一种编译器，已实现用“软线路”将速度提高100倍。

信息安全领域也有进化论倾向，在IDS(入侵监测系统)设计和防病毒软件设计中都希望系统具有自我进化能力——免疫系统，以对付新的、未知的入侵事件和病毒。密码设计也不例外，希望密码系统能够通过学习和进化具有应付未知攻击的能力。演化密码的提出是很有意义的，如能成功将给密码的研究产生巨大影响[15]。

目前见到的有关信息安全方面所有涉及进化论思想的已有工作还是很初步的，还都是利用已有的密码学知识，形成一些准则和预定目标，去寻求满足约束准则、达到预定目标的解。这似乎还没有超出已有的概念。

如何才算真的具有进化能力？我想，最基本的应当是系统能够利用已有的知识和新的数据产生出新的知识，这才是生物能够进化的根本条件。当然，要能设计出这样的密码系统，需要我们作长期不懈的努力，特别是要从更基本的理论上进行深入的研究。

5　指纹识别与身份认证

原来用于军事和法律中的生物身份识别技术开始走向民用，如用于电子商务和移动电子商务。其主要优点是依赖于生物特征而减少了对于密码的依赖，特别是绕开了密钥管理上的一些难题。生物特征包括动态的，即训练的行为和静态的，即自然属性。

基于学习训练的方法有：语音、手书和击键图样识别。基于自然特性的方法有脸型、视网膜、虹膜、手型、指纹等。显然一些基于步态、体味、DNA等的识别还没有在联机系统中实用。指纹识别技术是生物统计特征身份识别技术中研究最多、应用最广的一种。传统的方法是按手印，得到指纹的镜象，对此图像进行处理，提取出用户的特征信息。新的图像方法用光学、光－电子、电子或热传感器实现。

美国NIST和FBI已经收集了大量犯罪事件和相应的档案材料制作了大型指数据库。这有助于开发、训练和评价指纹识别算法。

这些技术的开发和推广应用需要标准化，以便能在运行环境下比较其性能、弱点等。只有解决了标准化问题，才有可能使这项技术能在大规模商业环境下实现网络化应用。

2002年5月22日本数学家Tsutomu Matsumoto发明了用透明胶和塑料伪造指纹，成功攻破了以指纹传感器构建的11种认证系统，每个系统在5次试验中有4次通过。

Bruce Schneier, CTO of Counterpane Internet Securi-

ty 的首席技术官和奠基人对此发表意见说，一个数学家而不是造假手印的专家，只用 $10 的材料，在厨房就可实现指纹认证公司专心经营的光敏技术产品！（http://www.counterpane.com/crypto-gram-0205.html）。这说明，信息安全决不能只靠一种技术来保证，应当采用多种技术手段实现。

6 信息安全技术人才培养

信息安全是高科技、高知识、高智能和高智商的争战。需要一流的人材、一流的技术、一流的产品。要组建信息对抗的机构和队伍，发展信息安全有关的高科技，加速人才的培养是首要的任务。

自 2001 年“9·11”事件后，美国政府大力加强信息安全人材的培养工作，每年拨款 1 100 万美元，在大学中设奖学金计划，用于培养计算机安全专家，向其 Cybercorps（信息部队）输送新成员[16]。此部队的任务是保护美国政府的信息技术基础设施的安全。这是一项高技术预备军官训练团（ROTC-Reserve Officer Training Corps）计划，在几个选定的大学之中挑选计算机科学和工程领域具有学士和硕士学位的学生进行两年训练，毕业后服务两年。计划于 2001 年秋开始执行。最初有 6 个大学参加：Tulsa, University of Idaho, Purdue University, Carnegie Mellon University, Iowa State University, Naval Postgraduate School。这些学校都在其计算机科学或工程系设有计算机安全课程计划，学校负责精心挑选学生，必须保证质量，否则后果严重。第一年有数千人申请，从中选了 54 名优秀学生，2001 年秋有 32 名，2002 年春有 22 名。下一学年将增加 4 个大学和 60 个新的奖学金名额。入选学生的所有学费、住宿费、书费等都由计划提供。每年，8 000 美元/大学生，12 000 美元/研究生。高年级大学生和第一年的研究生可以申请。选中者在暑假可以被资助去联邦政府或军队中进行计算机安全的实习。毕业后可以接触敏感的网络信息。

“9·11”事件像是世界上首次赛伯战争（Cyberwar）的开始，美军在 1997 年曾进行过一次作为 Eligible Receiver 一个组成部分的模拟事件的军事演习，用来检验国家对赛伯攻击（Cyberattack）的准备，国家安全局雇用了 35 名黑客向国防部的 40 000 个计算机网络进行入侵攻击。演习结束时，黑客获得 16 个网络的根级接入权，足以使几个主要城市断电，并能控制一艘海军巡洋舰。5 年以后开始的 Cybercorps 培养人材的工作意在使这类事件不再会发生。

我国对于信息安全和密码人才的培养也给予了足够的重视。1989 年在我国一些高校和研究机构设立了密码学硕士点，1993 年又设立了博士点。目前我国有几个硕士点和 3 个博士点（西安电子科技大学、郑州解放军信息工程大学和北京邮电大学）。1997 年 5 月 14—17 日在无锡召开了全国高校工科本科专业目录研究和修订会议，按照减少专业类，拓宽专业面向、柔性专业方向的原则，将我国 18 类 151 个工科专业合并成 16 类 60 个专业，并增设一类专业（生物技术与工程）和新增 4 个专业（生物技术与工程、信息网络对抗、粒子能武器、安全技术与工程）。此外，还提出专业面向更宽的引导型目录专业 14 种。这是一项非常重要的决策，对于提高我们的教育质量，培养适应不断变化的社会需求的人才有深远的影响。

增加的信息对抗专业，已有多所大学从 2000 年开始招收本科生。2001 年经教育部批准武汉大学率先开始招收信息安全专业的本科生，2002 年初批准 18 所、年末又批准 12 所院校招收信息安全专业的本科生。由此可见，我国对信息安全人才需求的迫切性和国家对培养这类人才的重视程度。

大学教育和人才培养有它的规律性，所谓“十年树木，百年树人”。从长远来看，专业的设置、人才的培养不能采取突击的办法。信息安全是一个重要的技术，但它是一个专业面较窄、涉及的知识面很宽、对学生要求又很高的专业。在短短的 4 年大学阶段要能培养出真正掌握信息安全基本知识和技术的专业人才不是一件容易的事。学生的负担会很重，能够承担此任务的大学生的比例不会很大，统一招生时又很难进行选择。因此，信息安全人才的培养方式应以研究生和培训班为主，前者培养高级专业人才，后者培养不同层次的应急专业人才。为了满足国家对信息安全人才的需求，可以在信息学科领域设置信息安全学科的硕士点和博士点。对一般大学生还是让他们学习那些基础性和适应性强的专业为好。

参 考 文 献

[1] Bennett C H. Quantum cryptography using any two non-orthogonal states. Physical Review Letters, 1992, 68:3 121—3 124.

[2] Bennett C H, Bessette F, Brassard G et al. Experimental quantum cryptography. Journal of Cryptology, 1992, 5(1):3—28.

[3] Bennett C H, Brassard G, Ekert A. K. Quantum cryptography. Scientific American, 1992, 267(10):50—57. 中译本：量子密码术.《科学》, 1993, 2:9—18.

[4] Ekert A K, Quantum cryptography bases on Bell's theorem. Physical

Review Letters, 1991, 67:661—663.
[5] Phoenix S J D, Townsend P D. Quantum cryptography: protecting our future networks with quantum mechanics (Invited Talk). in Cryptography and Coding, C. Boyd(Ed.), 1995, 112—131.
[6] Mullins J. Quantum physics spins off marketable Products-unbreakable encryption key is one of first new devices. IEEE Spectrum, 2002, 21—22.
[7] Mullins J. Making unbreakable code. IEEE Spectrum, 2002, 5:40—45.
[8] Shannon C E. A mathematical theory of communication. Bell System Technical Journal, 1948, 27(4):397—423.
[9] Detto W L, Lenstra A K. 驾驭混沌.《科学》, 1993, 40—46.
[10] Huang, 黄显高. 混沌保密通信中的非线性动力学问题研究. 西安交通大学博士学位论文, 2001, 10.
[11] Riezenman M J. The ABCs of IEEE 802.11. IEEE Srectrum, 2002, 39(9):20.
[12] Weinstein, Steve. The mobile Internet: Wireless LAN vs. 3G cellular mobile——An invited commentary. Comm. Mag., 2002, 40(2): 26—28.
[13] Agarwal A. 原始计算法. 计算机专题报告——氧工程.《科学》, 1999, 11:4—7.
[14] Dertouzos M L. 计算的未来. 计算机专题报告——氧工程.《科学》, 1999, 11: 8-11.
[15] Zhang, 张焕国, 冯秀涛, 覃中平等. 演化密码与DES密码的演化设计.《密码学进展——CHINACRYPT'2002》, 电子工业出版社, 2002, 8:88—95.
[16] Kushner D. Standing guard over cyberspace-a new U.S. Program trains students in computer security, in exchange for government service. IEEE Spectrum, 2002, 68—70.

DEVELOPMENT OF INFORMATION SECURITY THEORY AND TECHNIQUE

Wang Yumin
(The State Key Lab on ISN, Xidian University, Xian, Zip code 710071)

Abstract In this report we introduce the development of information security theory and technique. The report includes six parts: quantum cryptography, chaotic cryptography, the developments of 802.11b WLAN, the evolutionary theory and information security technique, fingerprint identification and identify authentication.

Key word cryptology, information security, training of information security experts

·资料·信息·

国家自然科学基金委员会杂志部将举办第二期科技论文写作高级研修班

随着我国科学研究水平的不断提高，基础研究与国际间的交流与合作日趋紧密。我国科研工作者参与国际重大科学计划、出席国际学术会议、申请各种基金、向国际知名期刊投稿，以及与同行或非同行的国际学术交流日益增加。因此，良好的沟通能力和技巧成为科学工作者的基本能力。

国家自然科学基金委员会杂志部将于2003年7月21—25日在北京和上海举办第二期科技论文写作高级研修班，课程内容的设计丰富与实用。授课教师是分别来自英国牛津、剑桥等著名学府的华人青年学者，他们分属不同学科，均有数次在国际知名学术期刊，如 *Nature*、*Science* 等上发表论文的实践经验。

详细信息请查阅国家自然科学基金委员会科学基金杂志部网页 http://pub.nsfc.gov.cn。

（科学基金杂志部 供稿）