doi: 10.3969/j.issn.1671-1122.2013.03.011

基于无线信道物理层特性的加密传输系统

黄橙，赵楠，郭开泰，郭万里
（西安电子科技大学，陕西西安 710126）

摘 要： 文章针对无线网络广播特性安全问题，以无线信道物理层特征互易性为基础，在借鉴现有信道特征密钥生成算法基础上提出“基于无线信道互易性三态量化的密钥提取算法”，并在Devkit8500A开发板上实现了应用该算法的安全通信。其次结合TF卡识别功能保证通信节点安全并利用GPS与Wi-Fi实现主动定位后台监控等功能，从而完成了一套基于信息论安全体系的利用无线信道物理层特性实现“一次一密”无线通信的安全解决方案，对无线通信安全研究具有积极意义。

关键词： 无线信道；物理层；三态量化；信息论；主动定位；一次一密
中图分类号： TP393.08 **文献标识码：** A **文章编号：** 1671-1122（2013）03-0040-05

The Confidential Transmission System based on the Physical Layer Characteristics of Wireless Channel

HUANG Cheng, ZHAO Nan, GUO Kai-tai, GUO Wan-li
(*Xidian University,Xi'an Shanxi* 710126, *China*)

Abstract: The paper, considering the secure problems of the broadcast nature of wireless network, drawing lessons from temporary key generation algorithm based on channel characteristics, based on the reciprocal physical layer characteristics of wireless channel, puts forward an innovative key generation algorithm of three-state quantization of wireless channel reciprocal characteristics, and accomplish a safety communication system which use this algorithm. Secondly, our system combines the secure transmission system with a bound personal identification card to assure the safety of communications and also utilize GPS and Wi-Fi to finish an active positioning daemon system to protect the communication terminal. In general, our work provides a “one-time pad”, based on information security system and the physical layer characteristics of wireless channel, wireless communication security solutions, which has positive meanings for the research of wireless network security.

Key words: wireless channel; physical layer; three-state quantization; theory of information; active positioning; one-time pad

1 作品背景

1.1 需求概述

无线通信技术正凭借其自身特有的多重优势在全世界通信领域飞速发展。较有线网络通信技术，无限通信不受线缆物理条件制约，地表条件的影响微乎其微，其服务范围广阔，无线网络中通信节点的设置与维护更为方便。然而，无线通信技术在带来种种便利的同时也带来了诸多安全问题。无线通信最显著的特点是使用具有开放性质的广播信道，由于无线通信是利用电磁波信号可以在自由空间中传播的特性进行数据传输，因此只要接收端在信号传递区域内，且具有相同接收频率就可能接收到所传递的信息，要将无线通信环境中传输的数据仅仅传达到个别信息接收端是不可能的。另一方面，由于无线设备多应用于移动环境并存在存储能力小、计算能力弱和电源能量有限、计算复杂度高的加/解密算法不适用等多方面的局限性，使得原来在有线环境下的许多成熟的安全方案和安全技术不能直接应用于无线环境。例如，传统防火墙对通过电磁波信号进行通信的网络攻击发挥不了作用。攻击者可以通过无线监听获取数据，并能够利用截获的数据反向推导分析出合法用户的信息及其认证模式，继而实施合法用户身份仿冒及其它恶意行为。因此，随着无线通信的发展和基于移动终端业务的爆炸式增长，有效利用无线通信信

收稿时间： 2012-12-15
作者简介： 黄橙（1991-），男，重庆，本科，主要研究方向：信息安全；赵楠（1990-），男，陕西，本科，主要研究方向：生物医学工程；郭开泰（1991-），男，陕西，本科，主要研究方向：测控工程与仪器；郭万里（1961-），男，陕西，高级工程师，主要研究方向：信息安全等。

道物理层资源，研究基于物理层资源的信息安全技术，探索能够有效提高无线通信系统安全性的新方法，具有深远的理论意义和巨大的实际应用价值。

1.2 现有方案调研

面对日益严峻的无线通信泄密问题，传统的解决方案只是通过加密技术加以解决。但对一个密码系统的评估，其中的一个重要方面就是在一定的合理假设下对其安全性的证明，每个密码系统在设计之初都必须要对其安全强度、实用性、效率等做通盘考虑。

当前，对加密技术模型进行安全证明的方法是用目前最优化的算法对该加密模型实施攻击所消耗的计算量，能够攻击成功要看攻击者的计算效率。若攻击密码模型所消耗的时间比加密技术所保护数据的保密期长，就可以认定该密码模型的设计是安全的。常见的公钥加密技术及对称密钥系统都是依靠相关计算模型设计。但是，理论上通过穷举攻击都可对以上密码技术进行破解，可即便是使用目前速度最快的计算机实施攻击也要少则数月多则上百万年时间才能破解的密码技术，可以被默认为是安全的模型。加密技术中还有一部分体制是通过数学计算方法作为安全性证明手段，该体制是将数学难解性问题应用于构建密码系统。典型的例子就是有限域上离散对数和大数分解等问题，解决这些问题目前还没有在计算效率或计算量方面可被人接受的算法。由于建立在安全模型基础上的加密机制的安全性无法得到证明，在难解问题计算中的风险也会随着加密技术的不断变化及计算资源功能的逐渐强大而发生变化。

与加密算法模型相对应的是信息论安全模型。该模型较前者有更强的安全模式，它是基于信息论的绝对安全性理论而建立：攻击者在时间无限且计算资源和攻击手段不受任何限制的前提下实施攻击，假如攻击者可以在较短时间内就将全部假设的密钥遍历一遍，也无法攻破基于信息论安全模型建立的加密技术。伴随着计算机技术的突飞猛进，理论上拥有近乎无限计算能力的量子计算机和 DNA 计算机可能在不远的将来诞生，对现有的加密算法模型产生重大的威胁。因此，基于信息论安全模型的加密技术将对未来的信息安全保护产生重要意义。

同时，传统的无线网络安全机制是基于安全中心分发加密密钥来提供保密和认证服务。但是在许多无线环境中（如移动通信），两实体间点对点的连接是在空中建立的，在这种情况下证书发放机构和密钥管理中心的可靠性很难得到保证。由于此种应用情景日趋普遍，无线通信双方不依靠安全基础设施而自主建立起安全加密体系的新方法迫切需要被发现。

基于前期调研的结果，为加强无线通信安全性，我组实现了一种基于信息论安全模型的并利用无线信道物理层特性实施的加密传输系统。

2 系统方案设计

2.1 系统方案概述

本系统以无线信道物理层特征互易性为基础，首先在查阅相关文献基础上对现有基于信道特征的密钥生成算法进行了 MATLAB 仿真实现和实际测试。在掌握第一手实验结果的基础上提出了“基于无线信道互易性三态量化的密钥提取算法”，并在以 TI 公司 AM3715 芯片为核心的 Devkit8500A 开发板上结合 Zigbee 通信模块，实现了探测提取信道特征、三态量化生成初始密钥、协商提取最终密钥的信道安全传输。其次结合身份信息绑定识别卡保证了通信端点的安全，并利用 GPS 与 Wi-Fi 实现主动定位后台监控等功能，从而完成了一套利用无线信道物理层特性实现“一次一密”的由点及面的加密传输系统（见图 1）。

图1 系统方案总图

2.2 系统方案测试

我们使用 MATLAB 对基于无线信道互易性的电平通过密钥提取算法进行仿真，以检验该算法的表现。该算法是以想要提取密钥的终端对无线信道进行连续探测作为初始的设计理念。由于存在物理层认证技术问题，我们假设敌对者在探测信道过程中没有进行主动攻击。仿真中主要考虑被动攻击这类第三方攻击模式。我们不考虑如中间人攻击等认证攻击，因为这需要 Alice 和 Bob 之间存在有明确的认证机制，并且这不能单靠提取秘密比特而得到解决。我们知道由于无线信道在空间上的快速不相关性，被动窃听攻击也不是很可行。我们考虑典型的室内无线环境情况下有 fd=10Hz。下面就开始介绍仿真实现该密钥产生的算法。

在仿真中，假设 Alice 为通信一方，Bob 为通信另一方。Bob 首先将训练序列（探测信息）发送给 Alice。Alice 收到信息后，迅速地将训练序列又回复给 Bob。两终端使用他们收到的训练序列计算出 64 点信道冲击响应，信道冲击响应的最高点就被用于作为此次探测的信道估计值，即送入密钥产生系统的 X 和 Y 的样本值。这里假设 Eve 企图捕获 Alice 发送给 Bob 的探测信息。

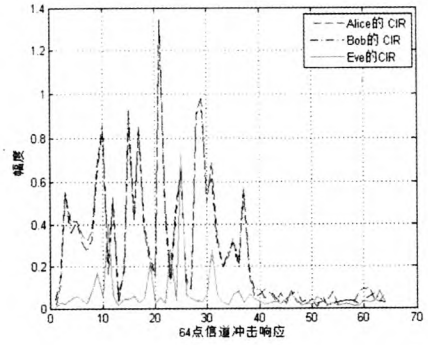

图2 从探测信号计算64点信道冲击响应

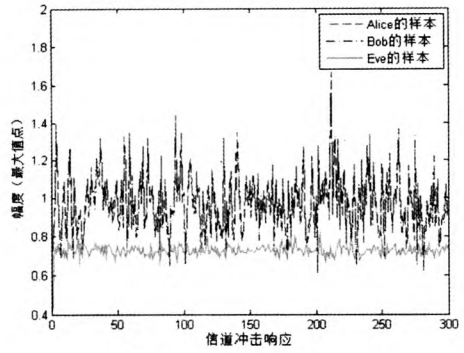

图3信道冲击响应峰值曲线

图 2 展示了Alice、Bob 和 Eve 从一次训练序列对中得到的 64 点信道冲击响应值的例子。从该图中可以看出 Alice 和 Bob 的冲击响应是十分相似的，而它们都和 Eve 的 64 点冲击响应有很大差别。

接着我们在图 3 中展示了计算得出的连续 300 个信道冲击响应值的最大值。从该图中可以看出 Alice 和 Bob 的曲线依然是十分相似的，而它们仍然与 Eve 冲击响应最大值的曲线有很大差别。

我们让 Alice 和 Bob 反复探测信道，得到 800 次信道估计，将未滤除阴影衰减的信道估计值送入电平通过密钥产生系统，并选择参数 m=3,a=1/8。最后产生出 44 比特的秘密比特。

Alice 产生的比特为：00100101000010010000001100010101001011100001

Bob 产生的比特为：00100101000010010000001100010101001011100001

Eve 产生的比特为：11011101001010100001101101110101000001000000

这个结果可以证明，Alice 和 Bob 所得的秘密比特出现很长的 0 比特串，且所得比特偏向于 0，而不是 0、1 的平均数，这是由于大尺度阴影衰落的影响，因此在将样本送入电平通过系统前，应先消除信道估计里的大尺度阴影衰落，仅留下小尺度衰落造成的变动。下面给出滤除阴影衰减后，由此系统得到的结果。

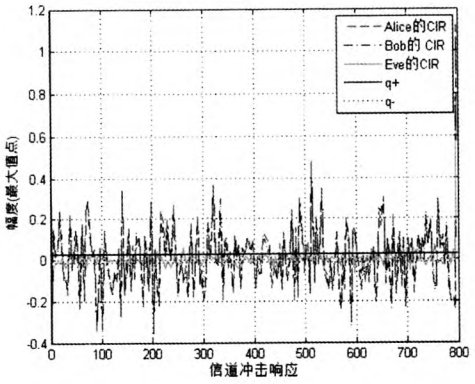

图4 滤除阴影衰减的样本值

滤除阴影衰减后，Alice、Bob 和 Eve 的信道冲击响应值如图 4 所示。这时将样本值送入电平通过密钥产生系统，并选择参数 m=3,a=1/8。最后产生出 52 比特的秘密比特。

Alice: 1001010101000010010000110001000100101010101001100111

Bob: 1001010101000010010000110001000100101010101001001100111

Eve: 1100000000100100011101000010100000000001101111010001

在信噪比为 10dB 的情况下，我们每秒进行 100 次探测，共持续 80 秒。得到的结果如下：

a=1/8、m=3 时，N=707 比特，秘密比特产生率为 8.84b/s。

a=1/8、m=4 时，N=231 比特，秘密比特产生率为 2.89b/s。

我们计算了信噪比为 0dB 时的误比特率，结果如下：

a=1/8、m=2 时，误比特率为 0.0304。

a=1/8、m=3 时，误比特率为 0.0258。

a=1/8、m=4 时，误比特率几乎为 0。

由此我们可以大概知道，当选 m 大于等于 4、a 大于 1/8 的时候，我们能以很小的误比特率利用电平通过算法在 Alice 和 Bob 之间产生密钥，速率约为 2.89b/s。而 Eve 通过窃听信道，经相同过程产生出的秘密比特与 Alice 和 Bob 之间的秘密比特是不相关的，这也表示出算法产生秘密比特的安全性。

3 系统原理与实现

3.1 无线信道物理层特性生成密钥部分

3.1.1 无线信道

信道是发射端和接收端之间传播媒介的总称，它是任何一个通信系统必不可少的组成部分。按传播介质分类，信道可分为有线信道和无线信道两大类，其中无线信道即是无线通信通过电磁波在空间中的传播来实现信息传递的路径。由于我组提出的密钥产生算法是基于无线信道物理层特性的量化，因此，在介绍“基于无线信道互易性三态量化的密钥提取算法”

前有必要简单介绍一下无线信道特性。

3.1.2 无线信道的传播特性

发射端与接收端之间的传播路径十分复杂，从简单的视距直线传播，到遭遇各种复杂地形（如建筑物、山脉和树叶等）导致的反射、绕射和散射都能够形成传播路径。由此可见，电磁波传播机制是多种多样的。

电磁波在自由空间中传播模型是分析无线信道特性的最基本的模型，多用于预测接收端和发射端之间在完全无挡隔的情况下接收端信号的场强。自由空间模型预测接收功率的衰减为发射端与接收端 (t-r) 距离的函数，模型中距发射端 d 处天线的接收功率由 Friis 公式给出：

$$P_r(d) = \frac{P_t G_t G_r \lambda^2}{(4\pi)^2 d^2 L}$$

其中，P_t 是发射端功率，$P_r(d)$ 是接收端功率，是 t-r 距离的函数；G_t 是发射端天线增益，G_r 是接收端天线增益；d 是 t-r 间距离，单位为 m（米）；λ 为波长，单位为 m；L 是与传播无关的系统损耗因子 ($L \geq 1$)。λ 与载频相关：$\lambda = \frac{c}{f}$，其中 f 为载频，单位是 Hz；c 为光速，单位是 m/s。两端天线增益与它的有效截面 A_e 相关，即：$G = \frac{4\pi A_e}{\lambda^2}$。有效截面 A_e 与天线物理尺寸相关，G_t 和 G_r 均为无量纲的量。综合损耗 $L(L \geq 1)$ 通常归因于传输线衰减、滤波损耗和天线损耗，当 L=1 时，表明系统中无硬件损耗。

3.2 身份信息绑定识别卡信息隐藏部分

当合法使用者需要保密通信时，需首先在上位机进行身份注册，并得到随机生成的身份识别 ID，同时系统在 TF 卡内写入隐藏有注册信息的认证文件，使用者取得与个人生物信息绑定的识别卡。当使用加密传输系统时，系统会检测该卡信息以决定是否给予使用者开启软件的权限。而后，要求使用者输入随机生成的身份识别 ID，用以双重认证，当盗用者三次输错身份识别 ID 后，系统启动数据自毁程序，删除并格式化信息绑定鉴别卡，保证系统安全。

3.3 主动定位后台监控部分

当用户通过身份信息绑定识别卡认证后，需要在“九宫格密码键盘”上输入认证密码。而当非法用户三次错误输入密码后，系统将自动退出并将系统所处位置的经纬度信息由 Wi-Fi 发送预警邮件给管理员，同时通过中国移动的 Fetion 服务发送短信至管理员手机，确保在第一时间发现风险。

4 硬件框图与软件流程图

我组设计实现的“基于无线信道物理层特性的加密传输系统”，以搭载 AM3715 芯片的 Devkit8500A 开发板为核心，上层运行 Android 操作系统，底层硬件以 UART、USB、TFT_LCD 为接口外扩 Zigbee、Wi-Fi、GPS 等功能模块（如图 5 所示）。实现了以无线信道物理层特性生成密钥功能为特色，可扩展身份信息绑定鉴别卡、改良型九宫格密码、主动定位后台监控防丢失等功能为辅助的无线通信安全解决方案。

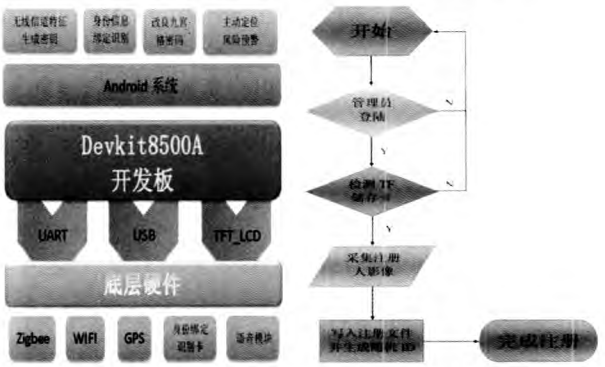

图5 系统硬件框图

图6 系统注册软件流程图

如图 6 所示，当使用者首次使用本加密传输系统，需在注册机上完成与个人信息绑定的注册认证，并凭借已透明写入注册信息的 TF 卡实现安全加密传输的后续操作。

如图 7 所示，当使用者在注册机上完成与个人身份信息绑定的认证后，即可凭借注册过的身份信息绑定识别卡使用基于无线信道物理层特性的加密传输系统。

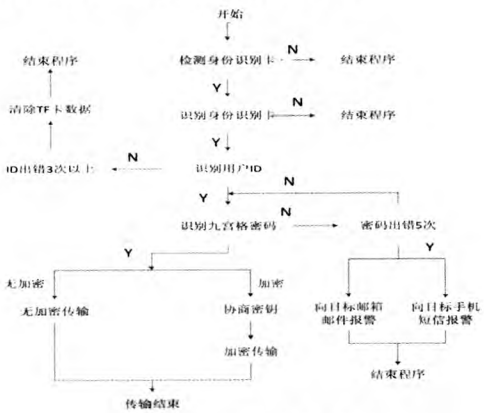

图7 系统安全通信软件流程图

5 系统测试

为检测本系统实际工作能力，我组在实际环境中对本系统进行了测试。同时根据测试数据，从密钥协商出错的概率、密钥生成速率和密钥随机性三个方面对系统做出了评估。测试系统也分为探测提取信道特征、协商提取初始密钥、量化与协商纠错三部分。如图 5 所示测试平台使用了两块 Devkit8500A 开发板完成，分别代表 Alice、Bob。无线数传芯片选择了 TI 公司的 CC2530 Zigbee 模块，上位机操作系统为 Android 2.2 系统。

为了得到基于信道特征的对称密钥，Alice 和 Bob 互发冗余数据包，并通过收到的数据帧得到当前信道环境下的信道特征检测值序列。为了使通信双方得到的检测值序列误差尽可能小，两次测量的间隔时间也应尽可能缩短。

实际系统测试中，我们编程实现了Zigbee自动重传无丢包传输机制，这样就确保了密钥协商双方在高度相关的信道特征检测序列里进行密钥协商。

本实验是在系统方案实际测试室内场地进行的。Alice、Bob距离为5米左右，物理位置上为直线。在Alice-Bob信道观测到的信号强度值如图8所示。

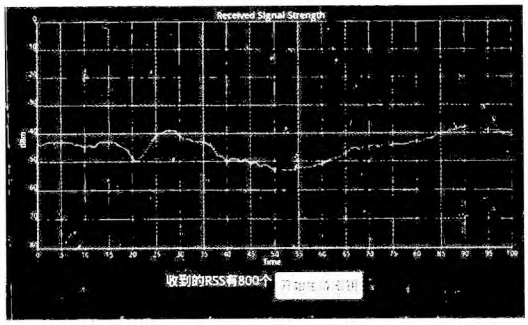

图8 静止协商密钥RSSI值波形图

从图8可以看出，在实际测试室内场地这一无线干扰相对较少的环境里，若Alice、Bob都处于静止状态，则信号强度变化幅度较小。上述实验中，信号强度的最大变化范围为25。由于信号强度变化较小，因此从信息论角度来看，信息熵也较小。因此在纯静止环境中原先的密钥协商算法几乎无法完成基于信道特征的密钥提取，但在引入我组提出的“基于无线信道互易性三态量化的密钥提取算法”后，即使在纯静止环境中也能顺利提取出密钥。

根据设计，在本实验中，Alice和Bob由实验者手持，实验者移动的速率约为每秒1米。此实验观测到的信号强度变化如图9所示。从图9可以看出，当通信双方移动时，信号强度的变化范围明显增大，达到了35。在移动环境中，信道特征的变化十分明显，信息熵大，更利于进行密钥提取设计中的后续步骤。

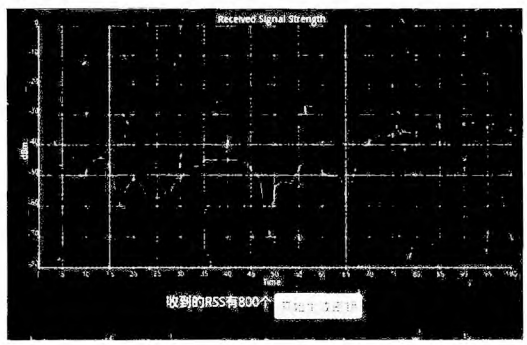

图9 移动协商密钥RSSI值波形图

针对一个用于生成密钥的系统来讲，首先想到的评价指标就是密钥生成的速率，即每秒钟能够生成的密钥的比特数，期望当然越快越好，但我们还需要考虑密钥协商出错的概率。由于Alice-Bob信道，信道特征检测值序列不完全相等。故我组提出了以特殊序列对代替信道检测序列全部数值协商密钥。增大特殊序列对的长度参数 m 会使得在量化阶段被最终采样的观测值减少，这也就降低了密钥生成的速率。因此我们在实际测试中对参数 m 进行了多次测试，并最终确定 m_0=6、m_1=6、m_x=8。

表1 协商对称密钥成功率测试结果表

	A端生成密钥	B端生成密钥
测试1	11111001	11111001
测试2	1x11010x	1x11010x
略去47组相同测试	…	…
测试50	11x1x101	1xx1x101

我们在多种情况下，对A、B双方根据信道检测序列生成对称密钥的成功率进行了50组测试。测试中可以顺利生成对称密钥46组，生成非对称错误密钥3组，未生成密钥1组（如表1所示）。可以认为，在硬件各接口接触良好的情况下，算法鲁棒性能良好。

我们选择了Maurer在文献[1]中给出的统计测试算法。Maurer的测试算法给出的值近似于平均熵，该值能很好地反映攻击者在暴力破解时候的难度。计算出本方案生成的密钥的P值为0.8902。可以看出，P已经接近理想随机序列的熵。由实验结果可见，我组“基于无线信道互易性三态量化的密钥提取算法”生成密钥的随机性良好，符合理论预测。

系统经测试，生成密钥功能实现良好，可实现无线通信安全加密传输。

6 结束语

本系统以无线信道物理层特征互易性为基础，首先在查阅相关文献基础上对现有基于信道特征的密钥生成算法进行了MATLAB仿真实现和实际测试。在掌握第一手实验结果的基础上提出了“基于无线信道互易性三态量化的密钥提取算法”，并在以TI公司AM3715芯片为核心的Devkit8500A开发板上结合Zigbee通信模块，实现了探测提取信道特征、三态量化生成初始密钥、协商提取最终密钥的信道安全传输。通过室内室外多种环境下系统功能测试，验证了三态量化算法鲁棒性良好，系统各功能指标均按计划实现，对基于无线网络物理层特性密钥提取的通信安全研究具有积极意义。（责编 杨晨）

参考文献：

[1] U. M. Maurer, A universal statistical test for random bit generators, Journal of Cryptology, vol. 5,pp. 89-105, 1992.

[2] 刘胜利．密码学中信息理论安全的研究 [D]. 西安：西安电子科技大学，1999.

[3] 张佳杰．基于导频的MIMO-OFDM信道估计技术研究 [D]. 天津：天津大学，2009.

[4] 韩旭．MIMO-OFDM系统信道估计算法的研究 [D]. 哈尔滨：哈尔滨工程大学，2009.

[5] 吴大焰．MIMO-OFDM系统中的信道估计和自适应传输技术研究 [D]. 江苏：东南大学，2008.

基于无线信道物理层特性的加密传输系统

作者： 黄橙， 赵楠， 郭开泰， 郭万里， HUANG Cheng， ZHAO Nan， GUO Kai-tai， GUO Wan-li
作者单位： 西安电子科技大学,陕西西安,710126

刊名： 信息网络安全
英文刊名： Netinfo Security
年，卷(期)： 2013(3)