广义频分复用系统在电力线通信中的运用

李琪林[1] 胡 苏[2] 武 刚[2] 周明天[3]
(四川电力试验研究院系统技术中心 成都 610072)[1]
(电子科技大学通信抗干扰国家重点实验室 成都 610054)[2] (电子科技大学计算机学院 成都 610054)[3]

摘 要 在现有的电力线通信系统(Power Line Communication,PLC)中,正交频分复用(Orthogonal Frequency Division Multiplex,OFDM)由于能够有效地消除电力线系统中的脉冲噪声干扰、多径时延干扰和群时延干扰,已成为一种主要的技术手段。OFDM技术尽管具有上述优点,但却存在高峰值功率、循环前缀导致的频谱利用率受限等问题。相应地,与OFDM具有不同设计思路的、基于成形滤波器的广义频分复用系统(Generalized Frequency Division Multiplex,GFDM)也就成为当前研究的热点。GFDM通过设计适合信道时延的成形滤波器,利用其时频聚焦性,可兼有抵抗字符间干扰(Inter Symbol Interference,ISI)和载波间干扰(Inter Carriers Interference,ICI)的能力,并可获得更高的频谱效率(无须循环前缀)。

关键词 电力线通信,广义频分复用,成形滤波器,时频聚焦
中图法分类号 TP393.02 **文献标识码** A

Generalized Frequency Division Multiplex for Power Line Communication System

LI Qi-lin[1] HU Su[2] WU Gang[2] ZHOU Ming-tian[3]
(Power Department,Sichuan Electric Power Test and Research Institute,Chengdu 610072,China)[1]
(National Communication Lab,UESTC of China,Chengdu 610054,China)[2]
(School of Computer Science and Engineering,University of Electronic Science and Technology,Chengdu 610054,China)[3]

Abstract Orthogonal frequency division multiplex(OFDM) is a good candidate for power line communication system, because it is effective against pulse noise, multipath delay and group delay. However, the drawbacks of the high peak-to-average power ratio and cyclic prefix lead OFDM system to have lower efficiency. Fortunately, Generalized Frequency Division Multiplex(GFDM) with good time-frequency localization can solve inter symbol interference(ISI) and inter carrier interference(ICI). Meanwhile, GFDM has higher spectrum efficiency because of no cyclic prefix.

Keywords OFDM, Offset QAM, Pulse shaping filter, Iterative channel estimation

PLC技术俗称"电力线上网"(Power Line Communication,PLC),是指利用电力线传输数据和话音信号的一种通信方式。以前该技术只作为长距离调度的通信手段,随着Internet技术的飞速发展,利用220V低压电力线传输高速数据的价值越来越为人们所重视。它具有不用布线、覆盖范围广、连接方便的显著特点,因此被认为是提供"最后一公里"解决方案最具竞争力的技术之一。

电力线通信业务需求快速增长,是近年来电力线系统通信关键技术、通信系统与网络架构不断演进和发展的推动力。但现有电力线通信技术提供的业务和服务能力仍无法满足泛在的、高速业务数据传输的电力线通信需求,导致这些问题的根本原因是电力线通信多接入技术的频谱利用率仍然很低。因此,面向未来的宽带电力线通信系统,需要研究适合未来通信频谱的高效调制编码、允许多种技术的多接入方法、智能资源管理与新型网络架构等关键科学技术。

此外,电力线不同于普通的数据通信线路,当作为一种数据传输的媒介遇到许多干扰时:首先,电力线上有许多不可预料的噪声和干扰源;其次,电力线通讯具有时间上不可控、不恒定的特点。为了克服各种干扰,电力线通信系统采用的调制技术主要是OFDM(正交频分复用)、DMT(多载波调制)、扩频及常规的QPSK,FSK等。为适应高速率的传输要求,多载波正交频分复用成为解决传输频带利用的有效方法。OFDM技术的主要思想是在频域内将给定信道分成许多正交子信道,在每个子信道上使用一个子载波进行调制,并且各子载波并行传输。但是,OFDM系统依然存在大时延环境等敏感问题,这将影响基于OFDM的电力线通信的稳定性;同时,OFDM技术的高峰值功率会影响基于OFDM的电力线通信功率的效率;此外,OFDM技术依赖循环前缀抵抗多径传

到稿日期:2009-10-26 返修日期:2010-01-20 本文受科技部十一五科技支撑项目-"现代服务业服务交互支撑平台"(项目编号:2006BAH02A0407)资助。

李琪林(1973-),男,博士,主要研究方向为电力自动化、电力线通信、可信计算技术;胡 苏(1983-),男,博士生,助教,主要研究方向为无线通信链路传输;武 刚(1975-),男,副教授,主要研究方向为MIMO、OFDM、信道建模;周明天(1939-),男,教授,主要研究方向为计算机网络、分布对象技术、并行分布处理。

播的代价是降低了系统频谱利用率，从而限制了数据传输速率。

若采取与 OFDM 不同的设计思路，可以基于非正交基函数和成形滤波器设计构成广义频分复用（Generalized Frequency Division Multiplexing，GFDM）多载波多址调制技术，包括正受到普遍关注的 OFDM/OQAM、非正交频分多载波调制与双正交频分多载波调制等方式。通过设计成形滤波器的时频聚焦特性来适合信道功率延迟特征与频偏特征，可无须添加循环前缀，并兼有抵抗字符间干扰（Inter Symbol Interference，ISI）和载波间干扰（Inter Carrier Interference，ICI）的能力[1]。根据正交方式及滤波器实现方法，GFDM 可以分为 3 大类：基于成形滤波器的 OFDM/OQAM（Offset-QAM）、广义多载波（Generalized Multicarriers，GMC）和非正交频分复用多载波调制以及双正交频分复用多载波调制。近来，OFDM/OQAM 系统已被提交至 IEEE 802.22 WRAN 和 3GPP LTE 的技术标准的草案中，实现复杂度成为 OFDM/OQAM 得到应用的主要阻碍。因此，作为对 OFDM 技术的补充和变革，包括 OFDM/OQAM、GMC、非正交、双正交等多种方式的 GFDM 具备成为未来新兴多载波调制技术的潜力。

1 系统描述

在传统 OFDM 系统中，由于时域通常采用严格的窗函数来控制符号间干扰，因此传统 OFDM 系统的成形滤波器呈现函数特性。通过观察函数发现，函数的旁瓣较高，相比于主瓣仅仅有 20dB 衰减，所以传统 OFDM 系统对于频率偏移非常敏感。到目前为止，具有良好时频聚焦特性的成形滤波器函数仅仅存在于实数域，因此基于成形滤波器设计的正交频分复用系统必须采用交错正交幅度调制方式（Offset QAM）。

OFDM/OQAM 系统通过采用具有良好时频聚焦特性的实数域成形滤波器，使发送信号对 ICI 和 ISI 具有较强的鲁棒性。与传统 OFDM 系统有所不同，基于成形滤波器设计的 OFDM/OQAM 系统满足实数域严格正交，代替了传统 OFDM 系统中的复数域正交。实数域正交基表示如下。

$$\langle g_{m,n} | g_{m',n'} \rangle_R = \mathrm{Re}\left(\int_R g_{m,n}(t) g^*_{m',n'}(t)\mathrm{d}t \right) = \delta_{m,m'}\delta_{n,n'} \quad (1)$$

在文献[2]中，作者提出一种基于 IFFT/FFT 模块的 OFDM/OQAM 系统低复杂度实现方法。OFDM/OQAM 发送信号表示为

$$s(t) = \sum_n \sum_{m=0}^{M-1} a^R_{m,n} g(t-2n\tau_0) j^{m+2n} e^{j2\pi m\nu_0 t} + j\sum_n \sum_{m=0}^{M-1} a^I_{m,n} g(t-(2n+1)\tau_0) j^{m+2n} e^{j2\pi m\nu_0 t} \quad (2)$$

式中，$a^R_{m,n}$ 和 $a^I_{m,n}$ 分别表示第 n 个符号、第 m 个子载波发送复数信号的实部与虚部，ν_0 和 τ_0 代表 OFDM/OQAM 系统子载波间隔和发送信号时间间隔，表示成形滤波器函数。以 $1/T_C = 2\tau_0/M$ 速率对发送信号 $s(t)$ 在时间间隔 $[nT_S - \tau_0, nT_S + \tau_0]$ 进行采样，发送信号可表示为

$$s_k[n] = g_k[n] * A^k_N(a^R_{m,n}) + g_{k-N/2}[n] * A^k_N(ja^I_{m,n}) \quad (3)$$

$$A^k_N(x_{m,n}) = \sum_{m=0}^{M-1} x_{m,n} e^{j\frac{\pi}{2}(m+2n)} e^{j2\pi\frac{nk}{M}}$$

$$s_k[n] = s[nM+k] = s(nT_S + kT_C)$$

$$g_k[p] = g[pM+k] = g(pT_S + kT_C)$$

在接收端，接收信号可以近似表示为

$$\tilde{a}^R_{m,n} \approx \mathrm{Re}\{ \sum_{l=-\infty}^{\infty} \sum_{k=0}^{M-1} r(lM+k) g^*_{m,2n}(lM+k) \}$$

$$\tilde{a}^I_{m,n} \approx \mathrm{Im}\{ \sum_{l=-\infty}^{\infty} \sum_{k=0}^{N-1} r(lM+k) g^*_{m,2n+1}(lM+k-M/2) \} \quad (4)$$

根据式(3)和式(4)，OFDM/OQAM 系统结构框图如图 1 所示。

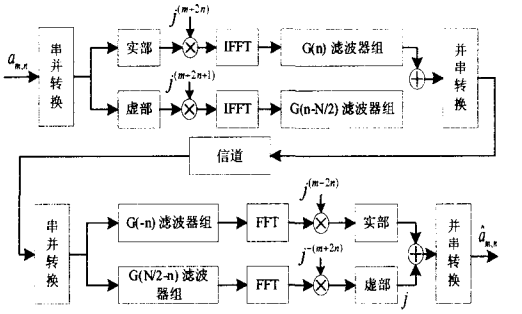


图 1 OFDM/OQAM 系统结构框图

通过观察图 1 可以看出，OFDM/OQAM 系统实现方式和传统的 CP-OFDM 系统结构非常相似，因此可以通过 IFFT/FFT 模块提高系统硬件实现效率。对比二者可以发现仍然存在一些细微不同：(1)输入复数信号会分成实部与虚部两个独立分支；(2)输入 IFFT 模块前，输入实数信号会通过变换因子重构输入信号虚实交替结构，从而满足实数域正交条件；(3)发送段 IFFT 模块后紧跟一个综合滤波器组，接收端在 FFT 模块前添加一个分析滤波器组，从而实现发送段成形滤波，接收端匹配滤波。

值得注意，与传统 OFDM 系统相比，OFDM/OQAM 系统将原始复信号转化为两个时刻的实信号发送，信号发射时间间隔缩短为传统 OFDM 系统的一半。从理论上而言，在相同的频率间隔下，OFDM/OQAM 系统与传统 OFDM 系统具有相同的频谱利用率。但在实际系统中，传统 OFDM 系统往往采用循环前缀来消除由多径效应带来的 ISI，所以 OFDM/OQAM 系统的频谱利用率要高于传统 OFDM 系统。

2 OFDM/OQAM 系统性能分析

结合上述分析可知，通过选择具有时频聚焦特性的成形滤波器，OFDM/OQAM 系统具有很好的时频聚焦特性。在文献[3]中，作者提出扩展高斯函数（Extended Gaussian Function，EGF）。该函数不仅具有高斯函数的时频聚焦特性，且能够保持滤波器相互严格正交（高斯函数具有很好的时频聚焦特性，但是基于高斯函数的成形滤波器之间不能满足正交条件）。EGF 函数表示如下。

$$z_{a,\tau_0,\nu_0} = \frac{1}{2}\left[\sum_{k=0}^{\infty} d_{k,a,\nu_0} \left[g_a(t+\frac{k}{\nu_0}) + g_a(t-\frac{k}{\nu_0}) \right] \right] \cdot \sum_{l=0}^{\infty} d_{l,1/a,\tau_0} \cos(2\pi l \frac{t}{\tau_0}) \quad (5)$$

式中，参数 a 表示扩展因子。此外，EGF 函数还有一个很重要的特性，该函数的傅立叶变换与函数具有相似的表达式，如

$$F(z_{a,\nu_0,\tau_0}) = z_{1/a,\tau_0,\nu_0} \quad (6)$$

式中，F 表示傅立叶变化。当 $a=1$ 时，EGF 函数的傅立叶变化等于其自身，所以该函数在时频域都具有相同的聚焦特性。EGF 函数如图 2 所示。

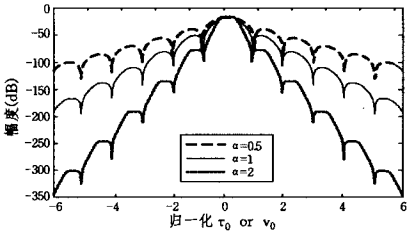


图 2　EGF 函数时频聚焦特性

观察图 2 可知，EGF 函数旁瓣快速衰落，所以 EGF 函数具有很好的时频聚焦特性。此外，在整倍数时间间隔(或频谱间隔)，EGF 函数会经过零点，因此 EGF 函数满足严格的正交条件。

在文献[4]中，作者提出的 OFDM/OQAM 系统结构可视为 GFDM 多载波调制的一种特例，其系统结构如图 1 所示。在图 1 中，$g(n)$是发射端成形滤波器，$\gamma(n)$是接收端匹配滤波器。经过数据交错(Data Stagger)以及不同频率调制后，发射信号时频域表示如图 1 所示。值得注意的是，通过 OFDM/OQAM 系统将原始复信号转化为两个时刻的实信号发送，信号发射时间间隔缩短为传统 OFDM/QAM 系统的一半。在相同的频率间隔下，OFDM/OQAM 系统由于发射信号不需要循环前缀，因此比传统的 OFDM/QAM 系统具有更高的频谱利用率。并且，OFDM/OQAM 的发射端和接收端依然保证了发送信号和解调信号的正交性原理。

除去 OFDM/OQAM 设计方式外，GFDM 系统还可采用非正交、双正交的收发滤波器组设计方式，或者采用退化的广义多载波设计方式。基于非正交的多载波调制方式中，发端滤波器组或接收端滤波器组都不能保证各自信号的正交性。但经过针对信道传输特性的设计后，能保证发端滤波器响应与信道传输响应、接收端滤波器响应卷积后的混合响应具有正交特性。广义多载波调制方式则是通过将所有频带划分为多个子带，对各个子带间进行成形滤波器设计，而在子带内仍采用正交设计，达到减少滤波器组数目、快速实现的目的。

通过选择具有时频聚焦特性的成形滤波器，GFDM 系统便具有很好的时频聚焦特性。在文献[5]中，作者提出扩展高斯函数(Extended Gaussian Function，EGF)。该函数不仅具有高斯函数的时频聚焦特性，且能够保持滤波器相互间严格正交。该函数表达式如下。

$$z_{\alpha,\tau_0,\nu_0}=\frac{1}{2}\left[\sum_{k=0}^{\infty}d_{k,\alpha,\nu_0}\left[g_\alpha\left(t+\frac{k}{\nu_0}\right)+g_\alpha\left(t-\frac{k}{\nu_0}\right)\right]\right]\cdot \sum_{l=0}^{\infty}d_{l,1/\alpha,\tau_0}\cos\left(2\pi l\frac{t}{\tau_0}\right) \tag{7}$$

为了表示成形滤波器的时频聚焦特性，可以通过模糊函数得到直观的效果。首先定义模糊函数如下。

$$A_g(\tau,\nu)=\int_R \mathrm{e}^{-j2\pi\nu t}g\left(t+\frac{\tau}{2}\right)g^*\left(t-\frac{\tau}{2}\right)\mathrm{d}t \tag{8}$$

从式(8)可发现，模糊函数直接反映了接收信号的解调增益和时延与频偏 v 的关系。当成形滤波器选用 EGF(α=0.265和 3.774)函数时，其模糊函数如图 3 所示。EGF 函数还有一个很重要的特性，即该函数的傅立叶变换与函数具有相似的表达式，如

$$F(z_{\alpha,\nu_0,\tau_0}(t))=z_{1/\alpha,\tau_0,\nu_0} \tag{9}$$

式中，F 表示傅立叶变化。当 $\alpha=1$，$\tau_0=\nu_0=1/\sqrt{2}$时，该函数的傅立叶变化等于其自身，所以该函数在时频域都具有相同的聚焦特性。

如图 3 所示，在发射端对成形滤波器进行预先设计，能使其良好的时频聚焦特性兼顾抑制多径时延和频率偏移的能力。进一步，这一思想可扩展成自适应 GFDM 系统，即在不同的时延和频率偏移的情况下，设计不同的滤波器特征，以适应信道的多径时延与频率偏移。一定程度上，图 3 所示的模糊函数反映了接收机解调增益对频偏和时延的鲁棒性。因此基于 EGF 函数的 OFDM/OQAM 系统不仅具备 OFDM 系统频谱效率高、抗脉冲噪声等优点，且能够抵抗多径干扰和多普勒频移影响。

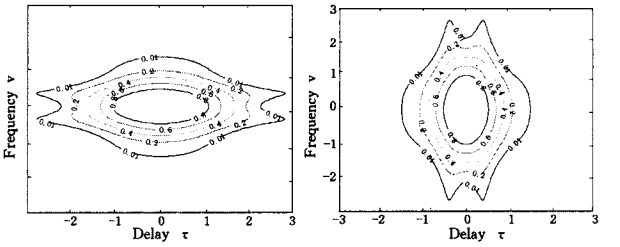
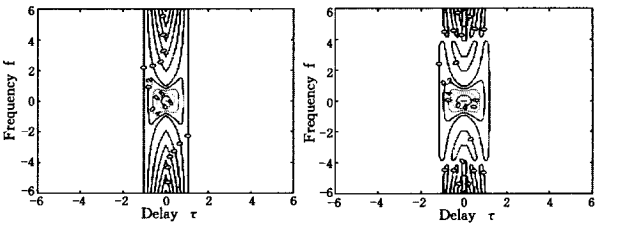
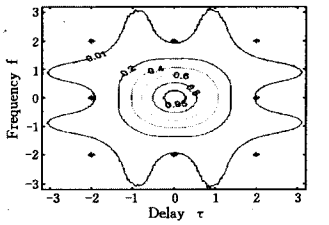


图 3　EGF 滤波器的模糊函数(α=0.265 和 3.774)

从时频聚焦的模糊函数来看，OFDM 的时频聚焦图案在时域上具有峰值下降较缓的特点，而在频域上稍微偏离峰值，这会使解调增益(模糊函数)快速衰减。这可以用图 4 的等高函数描述。



(a)没有前缀的 OFDM　　(b)有前缀的 OFDM(CP=1/5)



(c)OFDM/OQAM

图 4

结束语　在目前的电力线通信系统中，作为对基于 OFDM 技术方式的补充和变革，基于成形滤波器设计的 OFDM/OQAM 系统具备成为未来新兴多载波调制技术的潜力。OFDM/OQAM 系统通过选取具有良好的时频聚焦特性的成形滤波器来消除符号间干扰和子载波间干扰等电力线通信环境下的典型信道影响，并且该系统没有添加循环前缀，从而进一步提高了其性能。

参 考 文 献

[1] Le Floch B, Alard M, Berrou C. Coded Orthogonal Frequency Division Multiplex[J]. Proceedings of the IEEE, 1995, 83(6): 982-996

[2] Jinfeng D, Signell S. Time frequency localization of pulse shaping filters in OFD/OQAM systems[C]// the 6th International Con-

ference on Information, Communications & Signal Processing. Singapore, 2007: 1-5

[3] Bölcskei H, Duhamel P, Hleiss R. Orthogonalization of OFDM/OQAM pulse shaping filters using the discrete Zak transform [J]. Signal Processing, 2003, 83(7): 1379-1391

[4] TIA Committee TR-8. 5. Wideband Air Interface Isotropic Orthogonal Transform Algorithm(IOTA)-Public Safety Wideband Data Standards Project-Digital Radio Technical Standards [S]. TIA-902. BBAB(Physical Layer Specification, Mar. 2003) and TIA-902. BBAD(Radio Channel Coding(CHC) Specification, Aug. 2003

[5] Lele C, Siohan P, Legouable R, et al. Preamble-based channel estimation techniques for OFDM/OQAM over the powerline[C]// IEEE International Symposium on Power Line Communications and its Applications. Pisa, Italy, 2007: 59-64

(上接第 74 页)

于 H_1 是随机预言，故等式成立的概率至多为 2^{-l_q}。对于 Pr(NQ)：设 $\alpha\equiv g^k \pmod p$，$\beta\equiv h_1^{k'} \pmod p$，$y\equiv T^x\equiv g^{tx} \pmod p$，但 $z_1\equiv h_1^{x'}\neq h^x \pmod p$。由于签名是有效的，根据签名验证可知，$\alpha\equiv g^s y^{-c} \pmod p$，$\beta\equiv h_1^s z^{-c} \pmod p$，从而有 $k=s-ctx$，$k'=s-cx'$，这样就得到 $H_2(m||g||T||y||z||\alpha||\beta)=c=(k-k')/(x'-t\cdot x)$。由于 H_2 是随机预言，因此，F 在全部 H_2 询问中找到上述 c 的概率至多为 $q_{H_2}\cdot 2^{-l_q}$。

综上可知，A 成功解决 CDH 问题的概率至少为 $\varepsilon-(\varepsilon_{short}+\Pr(NH_1\cup NQ))=\varepsilon-(q_{sig}\cdot(q_{H_0}+q_{sig})\cdot 2^{-l_m}+q_{sig}\cdot(q_{H_1}+q_{sig})\cdot 2^{-l_r}+q_{sig}\cdot(q_{H_2}+q_{sig})\cdot 2^{-3l_q}+2^{-l_q}+q_{H_2}\cdot 2^{-l_q})$。

运行时间分析

A 的运行时间就是 F 的运行时间与群 $G_{p,g}$ 中的许多模指数运算时间之和。注意到一次 2 个指数幂乘运算大约相当于 1.2 次指数运算，从而运行时间为 $(q_{H_1}+4\cdot q_{sig})\cdot C_{exp}(G_{p,g})$。

因此原假设与 CDH 假设相矛盾，证毕。

4.2 协议的阈下封闭性

除了验证公钥 y 和 T 等公共参数外，接收者唯一能够获得的是签名消息$(m,(z,r,s,c))$，因此，签名者要传递阈下信息必须以签名(z,r,s,c)为载体。

由交互协议可以看出：尽管由 S 执行 $h_1=H_1(m||r)$，但他由于不知道 k_w 和秘密参数 t 的信息，因此不能控制 $r(\equiv y^{k_w^{-1}} \pmod p)$的取值，也就不能控制 h_1 的取值，而 $z_1\equiv h_1^x \pmod p$，$z\equiv z_1^t \pmod p$，因此也不能控制 z 的取值，从而不能控制 $c=(H_2(m||g||T||y||z||\alpha||\beta))$的取值。另外，尽管 S 能够得到 $\alpha(\equiv g^{k_A k_w} \pmod p)$，$\beta(\equiv h_1^{k_A k_w} \pmod p)$和 $\theta(\equiv c\cdot t\cdot k_w^{-1} \pmod q)$，但他由于不知道秘密参数 t，因此以不能获得关于 k_w，g^{k_w} 的任何信息，直至 W 完成最终签名之前，S 对 k_w，g^{k_w} 都是一无所知，因而不能控制 $s(\equiv k_w\cdot s' \pmod q)$的取值。特别地，如果 S 在 Step4 不使用 W 生成的 r，W 可以在签名生成时检测出来，从而终止协议。

由以上分析可知，发送者不能传送任何阈下信息给接收者，因此该协议封闭了由参数的随机性所引入的阈下信道。

4.3 计算复杂度及通信量

比起模指数运算，模乘和模加等运算的复杂度可以忽略，因此仅考虑模指数运算的复杂度。在本文的协议中，签名者和看守分别执行 2 次和 3 次模指数运算(不计预计算)，各进行 5 次数据传递，以此代价首次实现了 EDL 签名方案中由参数的随机性所引入的阈下信道的完全封闭，并确保了协议在 RO 模型中是安全的。

结束语 EDL 数字签名方案有着规约很紧的安全性证明，受到了业界的广泛重视。本文首先构造了 EDL 签名中的阈下信道，说明了 EDL 签名方案确实存在不足。接着，设计了一个交互式阈下信道封闭协议，它完全封闭了 EDL 签名中由参数的随机性所引入的阈下信道。基于 CDH 问题的困难性假设，在 RO 模型中证明了新协议是安全的。在新协议中，签名者签署的消息必须经过看守的审批方能生效。将来的目标是设计更有效的阈下信道封闭协议。

参 考 文 献

[1] Simmons G J. The 'prisoners' Problem and the Subliminal Channel[C]// Advances in Cryptology, Proc. Crypto'83. Springer Verlag, 1984: 51-66

[2] 董庆宽，肖国镇. 阈下信道分类及边信息协商问题研究[J]. 计算机科学，2004，31(5)：103-106

[3] Simmons G J. Subliminal Channels: Past and Present[J]. European Transactions on Telecommunications, 1994, 4(4): 459-473

[4] Simmons G J. Subliminal Communication Is Easy Using the DSA[C]// Proc. of Eurocrypt 93. 1994: 218-232

[5] Simmons G J. The Subliminal Channel and Digital Signature[C]// Advances in Cryptograph-Eurocrypt'84. Springer-Verlag, 1985: 364-378

[6] Xie Yuhua, Sun Xingming, Xiang Lingyun, et al. A Security Threshold Subliminal Channel Based on Elliptic Curve Cryptosystem[C]// Proceedings-2008 4th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, IIH-MSP. 2008: 294-297

[7] Kobara K, Imai H. On the Channel Capacity of Narrowband Subliminal Channels [C] // Proc. of the Second International Conference on Information and Communication Security. Berlin: Springer-Verlag, 1999: 309-324

[8] Goh EJ, Jarecki S. A Signature Scheme as Secure as the Diffie-Hellman Problem[C]// Biham E, ed. Advances in Cryptology-EUROCRYPT 2003. LNCS 2656. Berlin: Springer-Verlag Publishers, 2003: 401-415

[9] Meng Tao, Wang Jianfeng, Sun Shenghe. Cover Communication Based on Subliminal Channel in Broadcast Multi Signature[C] // Proceedings-2008 4th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, IIH-MSP. 2008: 309-1311

[10] Bellare M, Rogaway P. Random Oracles Are Practical: A Paradigm for Designing Efficient Protocols[C] // Proc. of the 1st ACM Conf. on Computer and Communications Security. New York: ACM Press, 1993: 62-73

[11] 陈伟东，冯登国，谭作文. 指定验证方的门限验证签名方案及安全性证明[J]. 软件学报，2005，16(11)：1967-1974