Schnorr签名中的阈下信道及其封闭方法

张应辉[1,2]，马 华[1]，王保仓[2]

(1. 西安电子科技大学理学院 西安 710071; 2. 西安电子科技大学计算机网络与信息安全教育部重点实验室 西安 710071)

【摘要】分析了阈下信道产生的原因及其在数字签名中的应用，对Schnorr签名中存在的宽带和窄带阈下信道进行了具体分析。设计了一个新的阈下信道封闭协议，新协议要求看守参与会话密钥的生成，确保会话密钥的随机性和隐私性。证明了新协议在保证签名者签名权力的前提下，完全封闭了Schnorr签名中由随机会话密钥所引入的阈下信道。新协议的安全性基于求解离散对数问题的困难性和哈希函数的安全性，在复杂度方面，签名者和看守各执行1次模指数运算。

关 键 词 密码学; 数字签名; 信息隐藏; 公钥密码学; 数据安全; 阈下信道

中图分类号 TN918 **文献标识码** A doi:10.3969/j.issn.1001-0548.2010.06.005

Subliminal Channels and Free Method in Schnorr Signature

ZHANG Ying-hui[1, 2], MA Hua[1], and WANG Bao-cang[2]

(1. School of Science, Xidian University Xi'an 710071;

2. Key Laboratory of Computer Networks & Information Security of Ministry of Education, Xidian University Xi'an 710071)

Abstract The reasons for the appearance of subliminal channels and their applications in digital signature schemes are analyzed. The wideband and narrowband subliminal channels in the Schnorr signature are discussed. And a new subliminal-free protocol is designed. In the new protocol, the warden participates in the generation of session keys in order to guarantee their randomness and privacy. It is shown that the protocol can completely close the subliminal channels existing in the random session keys in the Schnorr signature scheme. In addition, the signature authority of the signer is guaranteed. The security of the proposed protocol is based on both the discrete logarithm intractability assumption and the existence of collision-free hash functions. To generate a signature, it only needs to perform one modular exponentiation for each of the signer and the warden.

Key words cryptography; digital signature; information hiding; public key cryptography; security of data; subliminal channel

阈下信道也称潜信道[1]，作为信息隐藏的一个重要应用，阈下信道可被合法用户用于传递秘密信息[2]，广泛应用于军事、电子商务等领域。然而，阈下信道具有隐藏通信事实的特点，因此犯罪分子也可用阈下信道传递信息而不被发现，对信息安全带来了很大的挑战。利用阈下信道传输的隐藏信息称为阈下信息。在如今对信息安全要求越来越高的时代，如何有效地封闭阈下信道，使之不能为敌所用，成为各种安全机构亟需解决的问题。

围绕阈下信道的建立和封闭这两个相互矛盾和制约的技术，信息安全界进行了深入的研究。目前，绝大多数签名体制中都可能存在阈下信道。文献[1]指出Ong-Schnorr-Shamir[3]、ElGamal数字签名算法中均存在阈下信道[4]。文献[5]在DSA数字签名算法中成功地建立了一个宽带阈下信道。文献[6-7]对窄带阈下信道进行了深入的研究，在该类信道中消息发送方的密钥受到保护。文献[8]对ElGamal数字签名算法中随机数的选取作了研究。文献[9]提出了封闭DSA数字签名算法中的阈下信道的一个协议，文献[10]对此作了深入的研究，并将其推广到身份认证，零知识证明和电子护照等应用系统中。文献[11]建立了一个失败终止式阈下信道，指出文献[9]中的协议并不能完全封闭阈下信道。文献[12]采用分割选择的方式进行封闭，使阈下信道容量尽可能地小，但仍不能实现完全封闭。近几年，针对NTRU签名方案中的阈下信道及其封闭方法，基于椭圆曲线密码体制的阈下信道[13]均已被提出，目前对Schnorr签名方案中阈下信道的研究主要集中在阈下信道的设

收稿日期：2009－05－11； 修回日期：2009－08－10
基金项目：国家自然科学基金(60803149)
作者简介：张应辉(1985－)，男，博士生，主要从事密码学与网络安全方面的研究.

计、容量、安全性和封闭问题上，尚无Schnorr签名中阈下信道的完全封闭协议。

本文对Schnorr签名中存在的宽带和窄带阈下信道进行了具体分析，指出Schnorr签名中不存在宽带阈下信道，并给出了窄带阈下信道的构造方法，设计了一个新的阈下信道封闭协议，实现了Schnorr签名中由随机会话密钥所引入的阈下信道的完全封闭。在新协议中，看守参与了会话密钥的生成，阈下发方即签名者就不能控制签名算法的输出，也就是说对消息的签名必须由阈下发方和看守共同完成。在该协议中，看守虽然参与了签名的生成，但不能伪造签名，从而保证了签名者的签名权力。该文的方案也可以看作是一个新的带审批权的签名方案，必须由看守和签名者合作才能对给定消息进行签名。

1　阈下信道与Schnorr数字签名

1.1　阈下信道

阈下信道的宿主是概率数字签名或认证算法。阈下信息的发方在会话密钥的控制下对待嵌入的阈下信息进行随机化，然后通过嵌入算法把阈下信息嵌入到公钥密码系统的输入或输出参数中。阈下信息的收方在完成数字签名中的签名验证后，使用提取算法对所嵌入的阈下信息进行提取。除收方外，任何其他人均不知道密码数据中是否有阈下信息存在[14-15]。

在概率数字签名或认证方案中，会话密钥可以随机选取，从而使得消息和签名并不是一一对应的。同一个消息在不同的会话密钥作用下可产生不同的数字签名，这就为阈下信道的存在提供了条件。阈下信息的收方可以根据这些不同的签名获取公开收方无法得到的阈下信息。

一般一个有 a 比特的签名，若其中 b 比特被用于抗伪造、防修改、防移植等，则剩余的 $a-b$ 比特可被用于阈下信道。若能以 $a-b$ 比特传送阈下信息，则称其为宽带阈下信道；若仅能以小于 $a-b$ 比特传送阈下信息，则称其为窄带阈下信道。

1.2　Schnorr数字签名方案介绍

系统参数：随机生成两个大素数 p 和 q，使得 q 是 $p-1$ 的素因子，且 p 和 q 的二进制长度分别至少为1 024 bit和160 bit，以保证有限域GF(p)的乘法群 $\mathrm{GF}^*(p)$ 上的离散对数问题是困难的，即给定 g 和 $h=g^x\in\mathrm{GF}^*(p)$，求解 x 是计算上不可行的。随机选取 $\mathrm{GF}^*(p)$ 上的一个 q 阶元素 g。系统的公开参数就是 (p,q,g,H)，此处 H 是一个哈希函数。

密钥生成：签名者A选取一个随机数 x，满足 $1<x<q$，计算 $y\equiv g^x \bmod p$，则A的公私钥对为 (y,x)。

签名过程：设 M 为A要发送给B的待签名的消息。

(1) 预处理过程

A选取一个随机数 k，满足 $1<k<q$，并计算 $r\equiv g^k \bmod p$。

(2) 签名生成

A计算 $e=H(M\|r)$，其中 r 为A在预处理中产生的。$M\|r$ 表示比特串 M 和 r 的级联。A再计算 $s\equiv k+x\cdot e \bmod q$。$(e,s)$ 即为A对消息 M 的签名，A将签名消息 (M,e,s) 发送给签名验证者B。

(3) 签名验证者B验证签名

当B获得A发送的签名消息 (M,e,s) 之后，计算 $r'\equiv g^s y^{-e} \bmod p$，$e'=H(M\|r')$，检验是否有 $e=e'$，若是，则 (M,e,s) 是A发送的有效的签名消息；否则拒绝该签名。

2　Schnorr数字签名方案中的阈下信道分析

2.1　宽带阈下信道

在Schnorr数字签名方案中，如果使用宽带阈下信道，则签名者A将待发送的阈下信息作为会话密钥 k 进行签名。阈下信息的接收方B如果要提取阈下信息，就要在接收端恢复出 k 的值，而由方案的描述可知，k 的值满足 $s=k+x\cdot e \bmod q$，由于B不知道A的私钥 x，也就无法计算出 k；如果接收者计算 $r\equiv g^s y^{-e} \bmod p$，试图由 $r\equiv g^k \bmod p$ 求 k 的值，这将面临求解离散对数问题。因此，B不能完成阈下信息的提取，从而不能构造宽带阈下信道。

2.2　窄带阈下信道

由于在Schnorr数字签名方案中，接收者B收到的签名消息为 (M,e,s)，他可以由 $r=g^s y^{-e} \bmod p$ 得到 r 的值，故可以选择 r 为阈下信息的载体，因此可以构造窄带阈下信道。阈下信息的收发双方可以事先约定一个加密算法E，将待传送的信息用E加密后的值作为阈下信息，规定 r 的某几位为采用E加密后的固定值，如果 r 满足要求，则发送签名，否则重复上述过程。在这种情况下，需要多次选择 k 值以获得满足要求的 r，要传送 l 位阈下信息，通常需要进行 2^l 次参数选择。

3 封闭协议的设计

已有的各种封闭协议，如针对DSA数字签名算法的采用分割选择技术的封闭协议[12]等，因为阈下发方可以控制签名算法的输出，而输出能被收方得到，在传输过程中看守不再对此进行修改，即签名的最终完成者是阈下发方，不能达到完全封闭的目的。基于此，令看守W参与签名的生成，但他没有伪造签名的能力，从而可在保证签名者签名权力的前提下，实现对阈下信道的完全封闭。产生Schnorr签名的一个新的交互式协议如下。

3.1 系统初始化阶段

看守W随机选取整数t，满足$0<t<q$，则$\gcd(t,q)=1$，计算$T\equiv g^t \bmod p$，保密t，公开T。W秘密选取两个大整数c和d，满足$cd\equiv 1 \bmod q$。签名者A随机选取整数x作为私钥，其中$1<x<q$，并发布其签名公钥为$y\equiv T^x \bmod p$。公开发布两个安全的哈希函数H_0和H。

3.2 协议执行过程

步骤 1 W选取随机数k_W，满足$0<k_W<q$，则$\gcd(k_W,q)=1$，计算$\alpha\equiv g^{k_W c} \bmod p$，发送$\alpha$给签名者$A$;

步骤 2 A选取随机数k_A，满足$0<k_A<q$，则$\gcd(k_A,q)=1$，计算$\beta\equiv \alpha^{k_A} \bmod p$，$h_0=H_0(M\|\alpha)$，发送$\beta$和$h_0$给$W$；

步骤 3 W计算$r\equiv \beta^{h_0 d}\equiv g^{k_W k_A H_0(M\|\alpha)cd}\equiv g^{k_W k_A H_0(M\|\alpha)} \bmod p$，发送$r$给$A$;

步骤 4 A计算$e=H(M\|r)$，发送e给W；

步骤 5 W计算$u\equiv ek_W^{-1}\beta^{-1} \bmod p$，$\theta\equiv u^{-1}t^{-1} \bmod p$，发送$\theta$给$A$;

步骤 6 A计算$s'\equiv k_A\theta+x\beta h_0^{-1} \bmod q$，发送$(M,s')$给$W$;

步骤 7 W先验证$h_0=H_0(M\|\alpha)$和$e=H(M\|r)$是否成立，若不成立，则终止协议；否则计算：

$$\begin{aligned}s&\equiv k_W\theta^{-1}h_0 s'\equiv\\&k_W k_A h_0+k_W\theta^{-1}x\beta\equiv\\&k_W k_A h_0+k_W xtu\beta\equiv\\&k_W k_A h_0+k_W xtek_W^{-1}\equiv\\&k_W k_A H_0(M\|\alpha)+xte \bmod q\end{aligned}$$

然后发送(e,s)给B;

步骤 8 (签名验证过程)，当B收到(e,s)后，计算$r'\equiv g^s y^{-e} \bmod p$，$e'=H(M\|r')$，检验是否有$e=e'$，若有，则$(M,e,s)$是$A$发送的有效的签名消息；否则拒绝该签名。

3.3 正确性证明

签名验证过程的正确性由以下分析保证。

(1) 当(e,s)是A对消息M的有效签名时，一定有$s\equiv k_W k_A H_0(M\|\alpha)+xte \bmod q$，从而：

$$\begin{aligned}r'&\equiv g^s y^{-e}\equiv\\&g^{k_W k_A H_0(M\|\alpha)+xte \bmod q}y^{-e}\equiv g^{k_W k_A H_0(M\|\alpha)}g^{xte}y^{-e}\equiv\\&g^{k_W k_A H_0(M\|\alpha)}T^{xe}y^{-e}\equiv g^{k_W k_A H_0(M\|\alpha)}y^{e}y^{-e}\equiv\\&g^{k_W k_A H_0(M\|\alpha)}\equiv r \bmod p,\end{aligned}$$

因此，$e'=H(M\|r')=H(M\|r)=e$

(2) 如果$e=e'$，则一定有(e,s)是A对消息M的有效签名。否则，有：$s\neq k_W k_A H_0(M\|\alpha)+xte \bmod q$从而：

$$r'\neq r \bmod p$$

$$e'=H(M\|r')=H(M\|r)=e$$

即找到哈希函数的一个碰撞，对所采用的安全的哈希函数来说是困难的。

4 分析

4.1 协议的安全性

(1) 对除看守之外的任何第三方是安全的

令$k=k_W k_A H_0(M\|\alpha)$，$X=xt$，则签名验证者最终得到的签名(e,s)可简单地表示为$r\equiv g^k \bmod p$，$e=H(M\|r)$，$s\equiv k+Xe \bmod q$，也就是普通的Schnorr数字签名。因此可以保证对除看守之外的任何第三方是安全的。

(2) 对看守也是安全的

看守选取的秘密参数主要有t、k_W，不知道x、k_A，在步骤7之前看守不知道待签消息M以及$H_0(M)$、x、k_A之间的关系，无从伪造，因而伪造的唯一机会是在步骤7，此时看守W得到如下方程：

$$s'\equiv k_A\theta+x\beta h_0^{-1}s'\equiv k_A\theta+x\beta H_0^{-1}(M\|\alpha) \bmod q \quad (1)$$

W想要伪造A的签名，有下面两种情况可考虑：

(1) W可以考虑在步骤5时选择值j_0、z_0，并计算$\theta\equiv u^{-1}t^{-1}j_0 z_0^{-1} \bmod p$，发送$\theta$给$A$，在步骤7以$k_W\theta^{-1}h_0 j_0$ $(=k_W z_0 tuH_0(M\|\alpha))$乘以式(1)得到：

$$\begin{aligned}s&\equiv k_W\theta^{-1}h_0 j_0\cdot s'\equiv k_W k_A j_0 h_0+k_W z_0 tux\beta\equiv\\&k_W k_A j_0 h_0+k_W z_0 txek_w^{-1}\equiv\\&k_W k_A j_0 H_0(M\|\alpha)+xtz_0 e \bmod q\end{aligned}$$

然后寻找消息M'，使其哈希值满足$H_0(M'\|\alpha)=j_0 H_0(M\|\alpha)$和$H(M'\|r^{j_0})=z_0 e$，计算$e'=z_0 e$，从而得到签名消息$(M',e',s)$。但是这相当

于寻找哈希函数的碰撞，对于所采用的安全的哈希函数来说是困难的，因此看守不能伪造。

(2) 如果W要伪造的消息M'的哈希值满足$H_0(M'\|\alpha)=j_0H_0(M\|\alpha)$，即$H_0(M\|\alpha)=j_0^{-1}H_0(M'\|\alpha)$，同时还满足$H(M'\|r^{j_0})=z_0e$，结合式(1)可得$s'\equiv k_A\theta+x\beta j_0H_0^{-1}(M'\|\alpha)\bmod q$，两边再乘以$k_W\theta^{-1}H_0(M'\|\alpha)$得到：

$$\begin{aligned}s\equiv{}&k_W\theta^{-1}H_0(M'\|\alpha)s'\equiv\\&k_Wk_AH_0(M'\|\alpha)+j_0k_Wx\theta^{-1}\beta\equiv\\&k_Wk_AH_0(M'\|\alpha)+j_0k_Wxtu\beta\equiv\\&k_Wk_AH_0(M'\|\alpha)+xtj_0e\bmod q\end{aligned}$$

可以适当地选取哈希函数H_0和H，使得对任何M'有$j_0\neq z_0$。为产生有效的签名，W必须求解关于z的方程$H(M'\|r^{z\cdot j_0})=zj_0e$，然后计算$s''=zs$，$e'=zj_0e$，从而得到签名消息$(M',e',s'')$。但是由于方程中存在指数项$r^{zj_0}$，使得求解$z$将面临群$\mathrm{GF}^*(p)$上的离散对数问题，因此看守不能伪造。

由上述分析可知，W不能伪造签名。既然W允许无害消息传递，则W就必须完成协议，从而完成正确的签名。

4.2 完全封闭性

除了验证公钥y，接收者唯一能够获得的是签名消息(M,e,s)，因此签名者要传递阈下信息必须以签名(e,s)为载体。由协议可以看出，尽管A能够得到α $(\equiv g^{k_Wc}\bmod p)$和θ $(\equiv u^{-1}t^{-1}\bmod p)$，但由于他不知道秘密指数$c$、$d$及秘密参数$t$、$u$，所以不能获得关于$k_W$、$g^{k_W}$的任何信息。直至$W$完成最终签名之前$A$都对$k_W$、$g^{k_W}$一无所知，因而也就不能控制$s$ $(\equiv k_W\theta^{-1}H_0(M\|\alpha)s'\bmod q)$的取值。另外，尽管由$A$执行$e=H(M\|r)$，但由于他不知道$k_W$、$g^{k_W}$的任何信息，因而不能控制$r$ $(\equiv g^{k_Wk_AH_0(M\|\alpha)}\bmod p)$的取值，也就不能控制$e$的取值；如果$A$在步骤4不使用$W$生成的$r$，$W$可以在步骤7检验出来，从而终止协议。

由以上分析可知，发送者不能传递任何阈下信息给接收者，因此该协议实现了由随机会话密钥所引入的阈下信道的完全封闭。

4.3 计算复杂度及通信量

本文只考虑模指数运算的复杂度，因为与模指数运算相比，模乘和模加等运算的复杂度可以忽略。本文所设计的协议中，签名者和看守各需执行1次模指数运算(不计预计算)，他们之间共需6次数据交互，首次实现了Schnorr签名方案中由随机会话密钥所引入的阈下信道的完全封闭.

5 结　论

本文分析了阈下信道产生的原因及其在数字签名中的应用，讨论了Schnorr签名中存在的宽带和窄带阈下信道，并设计了一个新的阈下信道封闭协议。新协议实现了Schnorr签名中由随机会话密钥所引入的阈下信道的完全封闭，严格地说是计算上完全封闭的，依赖于离散对数问题的困难性假设和哈希函数的安全性。另外，新协议中签名者签署的消息必须经过看守的审批盖章方能生效。其他类型数字签名体制中阈下信道的构造及其封闭问题有待进一步研究。

参 考 文 献

[1] SIMMONS G J. The ‘prisoners’ problem and the subliminal channel[C]//Advances in Cryptology, Proc Crypto’83. Berlin: Springer-Verlag, 1984: 51-66.

[2] LI Wei, LI Gang, XIN Xiang-jun. Digital signature scheme with a (t,l) threshold subliminal channel based on RSA signature scheme[C]//Proceedings 2008 International Conference on Computational Intelligence and Security. Suzhou: IEEE, 2008: 342-346.

[3] ONG H, SCHNORR C P, SHAMIR A. An efficient signature scheme based on quadratic equations[C]// Proceedings of the 16th Annual ACM Symposium on Theory of Computing. Washington: ACM, 1984: 208-216.

[4] SIMMONS G J. The subliminal channel and digitalsignature [C]//Advances in Cryptograph-Eurocrypt’84. Berlin: Springer-Verlag, 1985: 364-378.

[5] SIMMONS G J. The subliminal channel in the U. S. digital signature algorithm(DSA)[C]//Proceedings of the 3rd Symposiumon State and Progress of Research in Cryptography-SPRC’93. Rome, Italy: [s.n.], 1993: 35-54.

[6] 张　彤, 王育民, 李真富. 牛顿信道的缺陷及其改进[J]. 通信保密, 2000, (2): 22-25.
ZHANG Tong, WANG Yu-min, LI Zhen-fu. The detects of Newton channel and the improvement[J]. Communication Security, 2000, (2): 22-25.

[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] YANG Jun, ZHOU Xian-wei, QIN Bo-ping. On the selection of random numbers in the ElGamal algorithm[J]. Journal of Electronic Science and Technology of China, 2006, 4(1): 55-58.

[9] SIMMONS G J. An introduction to the mathematics of trust in security protocols[C]//Proceedings of Computer Security Foundations Workshop VI. Franconia, NewHampshire: IEEE Computer Society Press, 1993: 121-127.

[10] DESMEDT Y. Abuses in cryptography and how to fight them[C]//Advances in Cryptology Proc of Crypto’88. Berlin: Springer-Verlag, 1990: 375-389.

[11] DESMEDT Y. Simmons'protocol is not free of subliminal channels[C]//Proceedings of the 9th IEEE Computer Security Foundations Workshop. County Kerry, Ireland: IEEE, 1996: 170-175.
[12] SIMMONS G J. Results concerning the bandwidth of subliminal channels[J]. IEEE Journal on Selected Areas in Communications, 1998, 16(4): 463-473.
[13] XIE Yu-hua, SUN Xing-ming, XIANG Ling-yun, 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. Harbin: IEEE, 2008: 294-297.
[14] SIMMONS G J. Subliminal channels: past and present[J]. European Transactions on Telecommunications, 1994, 4(4): 459-473.
[15] SIMMONS G J. Subliminal communication is easy using the DSA[C]//Proc of Eurocrypt 93. Berlin: Springer-Verlag, 1994: 218-232.

编 辑 税 红

(上接第819页)

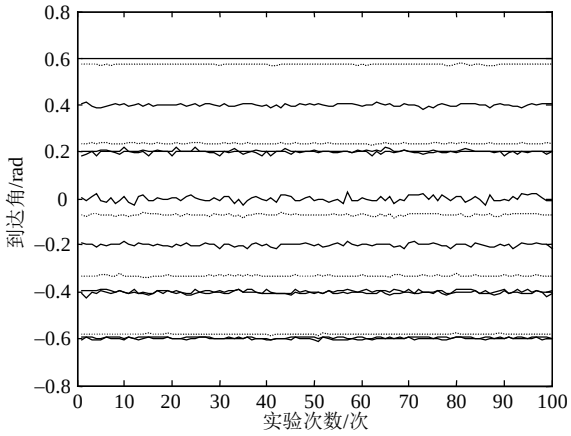

图3 7个信号源时本文方法和常规方法100次试验的估计结果比较

4 结 论

与针对单一的循环或非循环信号源的阵列信号处理不同，本文研究了循环和非循环混合信号源的波达方向估计问题和这两种信号源的识别问题，利用混合信号源的子空间特性推导并提出了增强型空间谱估计方法，该方法不仅具有较高的分辨率，容易识别该两种信号源，而且具有较强的信源过载能力。

参 考 文 献

[1] CHARG P, WANG Y, SAILLARD J. Non circular sources direction finding method using polynomial rooting[J]. Signal Processing, Elsevier Science Publishers, 2001, 81: 1765-1770.
[2] PICINBONO B. On circularity[J]. IEEE Trans SP, 1994, 42(12): 3473-3482.
[3] PICINBONO B, CHEVALIER P. Widely linear-estimation with complex data[J]. IEEE Trans SP, 1995, 43(8): 2030-2033.
[4] ABEIDA H, DELMAS J P. Stochastic Cramer-Rao bound of DOA estimates for non-circular Gaussian signals[C]//IEEE International Conference on Acoustics, Speech, and Signal Processing. [S.l.]: IEEE, 2004.
[5] CHARGE P, WANG Y, SAILLARD J. A root-music algorithm for non circular sources[C]//IEEE International Conference on Acoustics, Speech, and Signal Processing. [S.l.]: IEEE, 2001.
[6] HAARDT M, ROMER F. Enhancements of unitary ESPRIT for non-circular sources[C]//IEEE International Conference on Acoustics, Speech, and Signal Processing. [S.l.]: IEEE, 2004.
[7] CIBLAT P, SERPEDIN E, WANG Y. A fractionally-sampling based frequency offset enhanced blind estimator for non-circular transmissions[C]//Conference Record of the Thirty-Sixth Asilomar Conference on Signals, Systems and Computers. [S.l.]: [s.n.], 2002.
[8] CIBLAT P, LOUBATON P, SERPEDIN E, et al. Performance of non-data aided carrier offset estimation for non-circular transmissions through frequency-selective channels[C]//IEEE International Conference on Acoustics, Speech, and Signal Processing. [S.l.]: IEEE, 2000.
[9] GALY J, ADNET C. Blind separation of non-circular sources[C]//Proceedings of the Tenth IEEE Workshop on Statistical Signal and Array Processing. [S.l.]: IEEE, 2000.
[10] WANG H, CHEN B. On the distribution of peak-to-average power ratio for non-circularly modulated OFDM signals[C]//Global Telecommunications Conference. [S.l.]: [s.n.], 2003.

编 辑 税 红