文章编号：1007-0249 (2006) 01-0098-06

# 一种新的混沌加密系统方案原理*

丘水生，　陈艳峰，　吴敏，　马在光，　龙敏，　刘雄英

（华南理工大学 电子与信息学院，广东 广州 510640）

摘要：文中讨论了混沌的不可预测性，论证了不可预测的混沌信号的产生方法，并对混沌加密和常规加密系统进行了对比。在此基础上，提出了一个混沌与常规加密级联的系统方案。本文的主要工作在于阐述新方案的原理，提出了发挥混沌系统的不可预测性在混沌加密中的作用和将混沌加密与常规加密方法结合起来的思想。分析表明，这是提高加密系统安全性的一个新的重要研究课题。

关键词：电路与系统；加密系统新方案；混沌保密通信；混沌密码学

中图分类号：TP271.62；O175.15；TN918.8　文献标识码：A

## 1　引言

1990 年以来，混沌通信和混沌加密技术成为国际电子通信领域的一个热门课题。国际著名刊物 IEEE Trans. Circuits Syst. I 先后出版了四期混沌方面的专辑[2~5]，Proceedings of the IEEE 也于 2002 年 5 月出版了混沌学在电子与通信工程中应用的专辑[6]，显示了混沌通信研究的重大进展。然而，时至今日，仍然有不少重要或关键的问题尚未解决。例如，文献[7~9]提出并讨论了许多重要问题，其中包括混沌的基本特性以及系统安全性等方面的问题。这些文献着重于混沌的数学基础和加密系统分析等方面的探讨。在本文中，将从物理系统和应用技术的角度出发，主要讨论混沌的不可预测性和混沌加密系统设计原理的一些重要问题，并提出了混沌加密与常规加密相结合的加密系统新方案。文中关于混沌的不可预测性等的讨论是本文的理论根据，尤其是强调了混沌的不可预测性以及混沌与伪混沌的区别。

## 2　混沌的不可预测性

混沌具有不可预测性在许多文献中都有明确的叙述。文献[10]中指出，混沌吸引子局部地起着噪声放大器的作用，一个小的起伏会导致相轨很快产生大的偏离；过去和将来（系统状态）没有什么必然的联系。从数学的角度来看，确定的系统的演化（运动）完全取决于其矢量场及初始条件[9]。按照物理的观点，各种不同的噪声和干扰所引起的扰动（perturbation）限制了测量精度[10]。因此，无时不在的随机扰动是初始条件复杂性的来源。由此可得出结论：混沌形成的原因在于其外因（初值复杂性）通过内因（内秉随机性机制）起作用，而这种机制包括相轨的发散性和空间分叉的存在[11,12]。由此可知，初始条件的复杂性是混沌类随机性和不可预测性的根源。

根据文献[7]中随机性的表述，可以给出定义：对于动态系统的一个变量和任意给定的时间 $t_0>0$，如果总可找到不大的时间间隔 $\Delta t_0>0$，而不可能找出这样的一个通用公式或算法：它可以用来进行由 $t_0$ 时的变量值确定 $t_0+\Delta t_0$ 时的值的计算，则该系统是不可预测的。由此定义可知，利用数字计算机对混沌系统进行仿真时由一个初始值所得的相轨不是该系统的解。换句话说，此时计算机及其算法所构成的系统不是原混沌系统的准确模型，问题在于丧失了初始值的随机性。然而，利用数字计算机对混沌系统进行统计分析所得结果能够反映混沌系统的统计特性[10]。这是数值仿真的两个完全不同的概念。

理论上，混沌的类随机性意味着混沌的不可预测性。但是，在应用学科中，“有一定的随机性”通

* 收稿日期：2004-07-30　修订日期：2004-09-16
基金项目：国家自然科学基金资助项目（60372004）；广东省自然科学基金资助项目（31445，20820）

常意味着可预测性。由于这两种概念的存在，不仅应该认为混沌的不可预测性是其主要特性，而且是比随机性更重要的特性。否则，可能导致概念上的错误。

## 3　不可预测的混沌序列的产生

本文认为，由某些硬件电路组成的物理系统（例如蔡氏电路和模拟 Lorenz 系统的振荡器等）所产生的连续混沌信号是不可预测的，而数字化处理器可将这种信号转换为不可预测的混沌序列。就是说，产生工程技术所需要的不可预测序列是可能的。

在随机序列和伪随机数产生的研究历史中，利用物理系统产生随机序列的方法没有得到重视。究其原因，一是因为气体放电管一类的物理器件缺乏描述方程，其波形瞬息即逝而不能重复，因而其随机性难于得到严格的证明；二是其随机性不够强，往往满足不了实际需要；三是不便于应用。显然，利用混沌来产生不可预测的（随机的）序列的方法并不存在这些困难。当然，这种方法的实现需要有严格理论和检验手段的支持。

由第 2 节的论述可知，一个便于应用的随机系统应该具有初始值的复杂性和合适的系统方程。由于由硬件实现的蔡氏电路等物理系统必然存在噪声（扰动），又有确定的系统方程，因而满足了产生不可预测信号的前提条件。文献[13]试图利用 Shil´nikov 定理来证明蔡氏电路是一个严格意义上的混沌系统，并得出了证明成功的结论。实际上，由于该定理的条件所要求的同宿相轨难于找到，其证明过程的部分叙述有些牵强。本文相信，文献[11]提出的混沌吸引子存在定理更容易应用于实际物理系统。本文强调，文献[11,12]中提出的“相空间分叉”是有助于理解混沌系统内秉随机性的重要概念。判定这类物理系统的数学方程具有混沌性质的仿真试验（检验）方法在文献中容易找到。要特别提及的是，文献[10]第 52 页中的图及说明提供了判定不可预测性的一个有用技术，前提是研究对象必须是物理系统。

在原理上，利用测量来检验实际混沌波形的不可预测性是可行的。通过测量和变换可得到系统的近似混沌序列。上述的不可预测性的定义可应用于这种序列的检验。另外在常规密码学中，有一种检测伪随机序列周期性的方法[14]。将这种方法应用于混沌序列将得到两种可能的结果：不存在周期性，或者偶然有周期现象但不规则地出现。这些结果都可以用来判定混沌序列的不可预测性，其根据是：具有初值随机性的系统产生的非周期波形是不可预测的。值得指出，实际波形的测量值有一定的误差，但混沌波形的近似仍然是混沌的。这种“有限精度”效应与产生伪混沌序列的数字仿真系统的具有实质性的不同。前者没有改变原有的初始值复杂性，其影响相应于连续频谱的局部改变，而后者则因丧失初始值复杂性必然输出可预测序列。由此可见，产生不可预测的密码流也是完全可能的。

## 4　混沌加密系统和常规加密系统

### 4.1　基本术语

1）常规加密系统：基于常规密码学，以离散值-离散时间方式运行的加密系统[14]。

2）公钥制加密系统：非对称加密系统。

3）混沌加密系统：采用不可预测的混沌信号的加密系统。它工作于连续时间或离散时间运行方式。

4）伪混沌加密系统：利用伪混沌密钥信号，或利用由初值确定的相轨演化作为加密算法的加密系统。在后一种情况下，可称之为伪混沌加密算法或伪混沌加密器，这类系统一般采用离散时间方式运行。

5）利用伪混沌的常规加密系统：将伪混沌信号（或算法）应用于常规加密算法的系统。

6）混合加密系统：由上述各种系统中的两种或多种组成。

### 4.2　保密系统应满足的基本要求

上述各种加密系统都应该满足相同的基本要求。这种要求可归结为四条[15]，其中之一是：系统的保密性不依赖于对加密体制或算法的保密，而依赖于密钥。应该指出，密钥信号产生器是可以不公开

的，一些涉及密码分析的文献（例如系统识别攻击的有关文献）往往采纳这一设计原则。这一点对于发挥混沌加密的优点特别重要。

### 4.3 混沌加密与常规加密原理的比较

扩散和混淆是由 Shannon 提出的密码系统设计的两个基本原理。扩散的作用在于将明文的统计特性散布到密文中去，实现方式是使得明文的每一位影响密文中多位的值。混淆则是使密文和密钥之间的统计关系变得尽可能复杂，使敌手无法得到密钥。混沌的轨道混合（mixing）特性（与轨道发散和初始值敏感性直接相联系）相应于常规加密系统的扩散性能[9]，而混合特性和混沌加密系统可采用的强非线性变换效果相应于常规加密系统的混淆特性。可见，在原理上，混沌加密器的扩散和混淆作用也可以达到高安全性的要求。

混沌加密器通常工作于连续值方式，而常规加密器工作于离散值方式，这是两者的主要差别。理论分析表明[9]，工作于后一方式的系统的某些性能优于采用前一方式的系统的性能。但是，决不能因为这种性能差别而得出混沌加密不能应用于具有高安全性要求的加密系统的结论。这种结论的片面性是明显的，因为这等于否定了不可预测的混沌信号在加密系统中的重要性。值得指出，混沌加密器也可数字化（第 3 节中已指出产生不可预测的密码流的可能性），而文献[8]并没有考虑这种方案。

### 4.4 常规加密系统

这种系统的原理在文献[14~17]中有详细的叙述，通常是指采用单钥体制的加密系统。单钥体制的加密方式主要有两种：明文消息按字符（如二元数字）逐位加密，称为流密码；将明文消息分组（含多个字符），逐组加密，称为分组密码。本文中说到常规加密器时，往往是指分组密码算法。

与混沌加密系统相比，常规加密系统的特点是：

1）建立了分析系统安全性和加密系统性能的理论；

2）密钥空间的设计方法和实现技术比较成熟，系统安全性好；

3）采用伪随机数作密钥；

4)采用离散值－离散时间运行方式,而系统性能会有某些优点；

5）可以得到明文-密文对。这是它可能被破译的关键原因。

### 4.5 混沌加密系统

凡是试图利用混沌（不是伪混沌）信号或系统的各种加密系统都属于这一类加密系统。其典型系统之一的原理框图如图 1 所示。它来源于文献[18]，但这里的“同步信号”方块在文献[18]中是“同步冲击信号”。作这一小改变是为了有较好的普遍性。编辑器的作用是形成时分的发送信号。扰频器使信号频谱复杂化。加密器采用一个 $n$ 次移位变换（详见文献[18]）。

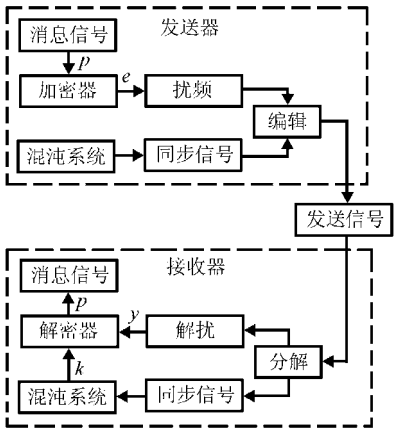



图 1 一种典型的混沌加密系统

与常规加密系统相比，这种加密系统的特点是：

1）复杂的密钥信号由简单的电路来产生；

2）利用由硬件实现的混沌系统。密钥信号是不可预测的。此时，不存在唯一对应的明文密文对，而与同一明文相应的是各不相同而不相关的密文；

3）采用连续值－连续（或离散）时间运行模式；

4）不少文献都未深入考察密钥空间的设计问题。利用不可预测的密钥信号时，混沌系统初始值不能作为密钥参数。在简单的混沌信号产生器中，可用作密钥参数的电路参数数目很少，因而混沌电路容易被识别。这是系统安全性差的主要原因；

5）系统安全性只能依靠有限的数值方法来检验；

6）若混沌密钥信号由数字仿真系统（例如计算机）来产生，则称为软件化混沌系统。这等于采用了一个伪混沌加密系统。现有文献中分析混沌加密系统时往往出现这种情况。

### 4.6　伪混沌加密系统

前面已提到了这种加密系统的基本特征。其主要特点在于系统的密钥信号或加密算法具有可预测性。从这个角度来看，它的安全性比不上混沌加密系统。目前，国际上报道的采用软件化混沌系统的加密器属于这一类。基于 INTERNET 的加密系统一般也属于这一类，它可分为三种：一是采用伪混沌流密码的系统；二是各种采用混沌调制的系统的软件化系统；三是以明文作为系统初值的伪混沌加密器。研究这三种系统的文献，有一部分深入考虑了密钥空间设计的问题[19]。

## 5　混沌加密的新方案

### 5.1　新方案的设计原理

综上所述可知，混沌加密系统的主要优点是利用了混沌信号的不可预测性，主要缺点是没有解决密钥空间的设计问题；常规加密系统的主要优点在于具有成熟的密钥空间设计技术，而且其安全性较容易评估，主要缺点在于明文密文对唯一对应而有可能被破译。根据两者的对比，就可得到如下的设计思想：

1）利用两类系统优点互补的原则（以一方的优点弥补另一方的缺点），可以构造一个级联系统，前级采用混沌加密器，后级采用常规加密器。这体现了将混沌加密和常规加密相结合的思想；

2）将上述级联系统的后级改为伪混沌加密器（或一个网络），其主要任务在于形成足够大的密钥空间（根据这一点，文献[20]提出了一种混沌－伪混沌级联加密方案）；

3）在混沌加密级中加设一个变换方块（下称相图变换），其作用在于增加其密文输出的相图的复杂和畸变程度，因而明显增强了混沌加密级的抗攻击能力；

4）硬件实现的混沌系统（密钥信号产生器）是不公开的，这意味着存在一个暗密钥（参数）空间，而实际系统中将采用新型的或复杂化的混沌产生器。

### 5.2　混沌加密与常规加密的级联方案

这种级联系统的典型方案原理图如图 2 所示。其发送机由两种加密器构成级联系统。前级有附加的相图变换器，其基本部分的原理与图 1 的系统相同，而混沌系统不公开。后级是带有 A/D 转换器的常规加密器，可以利用现成的加密算法，例如 DES 或 AES[14]。显然，系统的密钥空间的设计和实现是有保证的。接收机的变换器具有反变换的功能。

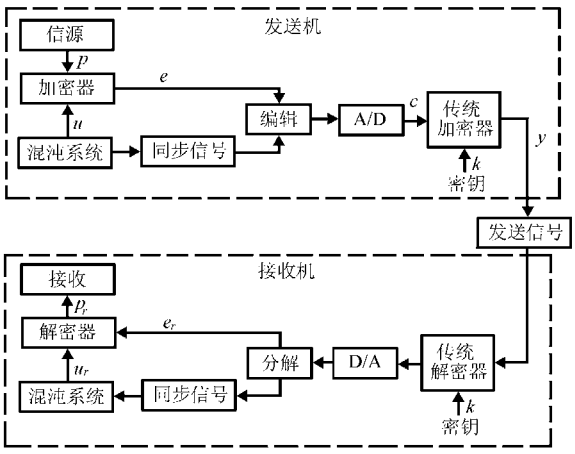



图 2　混沌与常规加密级联系统的典型方案

本系统的主要优点及安全性分析：

1）将混沌加密器与常规加密器相结合，两种加密器的优点可以互补，使整个系统的抗攻击能力明显高于其中的任一加密器；

2）除了穷举攻击之外，常规加密算法的所有已知攻击方法的基本条件是某些唯一对应的明文密文对[14]。由于采用硬件实现的混沌系统而前级密钥信号 $u$ 是不可预测的，因而其输出 $e(t)$是随机变化的，故不存在唯一对应的明文密文对。常规加密器的输入 $c(t)$是 $e(t)$经过相图变换而来的，因而比 $e(t)$有更强的随机性，因此对于后级加密器来说更加不可能有唯一对应的明文密文对。这样，上述的已知攻击方法在原理上不可能击破常规加密器。由此可见，前级优点弥补了后级的弱点，而显著增强了后级的安全性；

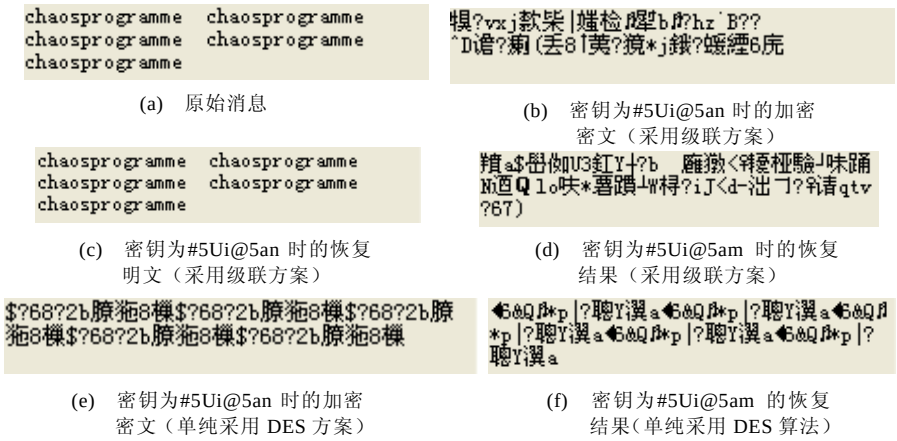
3）在上述的后级不可击破的情况下，要获得其输入信号 $c(t)$是不可能的。这样，要得到相图变换的输入信号就更加困难。因此，目前已知的利用频谱分析、系统识别等的破译方法对于前级的攻击就无能为力了；

4）这一方案的安全性能容易评估。

综上所述，可作出一个猜测：对于这种级联加密系统来说，不存在比穷举攻击（唯密文攻击）更加有效的破译方法。其关键在于，不可预测的混沌密钥信号是“过去和将来没有什么必然联系”的一种信号，相当于“密钥”无限多次变化的过程。值得指出，上述级联方案可以有一些不同的变形。例如，混沌加密级可利用硬件实现的映射方程，也可采用流密码模式，并且混沌信号产生器可以输出不可预测的混沌数字信号（见第 2 节有关叙述）。

## 6 新方案的初步仿真结果

为验证新方案的可行性，对混沌与常规加密级联方案进行了初步的仿真。其结果如图 3。




(a) 原始消息　(b) 密钥为#5Ui@5an 时的加密密文（采用级联方案）

(c) 密钥为#5Ui@5an 时的恢复明文（采用级联方案）　(d) 密钥为#5Ui@5am 时的恢复结果（采用级联方案）

(e) 密钥为#5Ui@5an 时的加密密文（单纯采用 DES 方案）　(f) 密钥为#5Ui@5am 的恢复结果（单纯采用 DES 算法）

图 3 新方案的初步仿真结果

由于图 2 所示的系统中采用的是具有强随机性的不可预测混沌加密信号，而数字计算机仿真过程缺乏硬件混沌信号产生器所具有的随机扰动，故常规仿真方法的应用会遇到新问题。因此，初步的仿真是对上述级联系统的一个变型进行的。其混沌加密级采用 Logistic 映射所产生的伪混沌序列，常规加密级采用 DES 算法。仿真采用 VISUAL C++，选用一段有重复消息的文档作为明文，所得结果示于图 3(a)~(d)。为了对比，图 3(e)~(f)给出了对单纯 DES 算法进行仿真的结果。从这些图可看出，当采用密钥为#5Ui@5an 加密、解密时，得到了正确的恢复明文，而采用有误差的密钥解密时得到全是乱码。可见，该级联系统能够正常工作。另外，当原始文档中有重复消息时，在级联系统分别得到的密文（图 3(b)）和乱码（图 3(d)）中未出现重复信号，但单纯 DES 算法的密文（图 3(e)）和乱码（图 3(f)）中均出现了与明文相对应的重复信号。这表明即使混沌加密级采用伪混沌信号，级联方案的密文的周期性与单纯 DES 算法的周期性相比是比较弱的。由这些结果可以预料，采用不可预测的混沌信号的级联方案即使同一明文重发多次也得不到任何明文密文对，因而通常的基于明文密文对的密码分析方法将会失效。

## 7 结论

本文论证了混沌系统的不可预测性的数学意义及其在混沌加密中的重要性。在此基础上论证了不可预测的混沌密钥信号的产生方法，对混沌加密和常规加密方法进行对比，并提出了利用混沌的不可预测性的级联混沌加密方案。分析表明，此方案具有很好的安全性。本文思路的出发点在于利用混沌密钥信号的不可预测性，而发挥混沌信号的不可预测性在加密系统中的作用和混沌加密与常规加密相结合是提高加密系统安全性的一个新的重要研究课题。

参考文献：

[1] Lorenz E. Deterministic non-period flow [J]. **J. Atmos. Sci.,** 1963, 20(3): 130-141.

[2] Chua. L O. Special issue on chaos [J]. **IEEE Trans. Circuits Syst.I,** 1993, 40(10,11).

[3] Kennedy M, Ogorzalerk M. Special issue on chaos synchronization and control [J]. **IEEE Trans. Circuits Syst.I,** 1997, 44(10).

[4] Kennedy M, Kolumbán G. Special issue on noncoherent chaotic communication [J]. **IEEE Trans. Circuits Syst. I,** 2000, 47(12).

[5] Kocarev L, Maggio G, Ogorzalerk M. Special issue on applications of chaos in modern communication systems [J]. **IEEE Trans. Circuits Syst. I,** 2001, 48(12).

[6] Martin Hasler, Gianluca Mazzini. Special issue on applications of nonlinear dynamics to electronic and information engineering [J].

**Proceedings of the IEEE,** 2002, 90(5).
[7] Brown R, Chua L O. Clarifying chaos : examples and counter examples [J]. **Int. J. Bifur. Chaos,** 1996, 6(2): 219-249.
[8] Dachselt F, Schwarz W. Chaos and cryptography [J]. **IEEE Trans. Circuits Syst. I,** 2001, 48(12): 1498-1509.
[9] Kocarev L. Chaos-based cryptography: A brief overview [J]. **IEEE Circuit and system Magazine,** 2001, 1(3): 6-21.
[10] Crutdhfield J. Chaos [J]. **Sci. Amer.,** 1986, 255: 46-57.
[11] Qiu Shui-Sheng. Study of existence and structure of chaotic attractors [A]. **Proc. Int. Symp. on Nonlinear Theory and Its Applications** [C]. Xi' an, 2002.
[12] 丘水生. 混沌吸引子的周期轨道理论研究(I) [J]. 电路与系统学报, 2003, 8(6).
[13] Chua L O, Komuro M, Matsumoto T. The double scroll family [J]. **IEEE Trans. Circuits Syst. I,** 1986, 33(11): 1072-1118.
[14] Stallings W. 密码编码学与网络安全：原理与实践 [M]. 杨明, 等译. 北京：电子工业出版社, 2001.
[15] 杨波. 网络安全理论与应用 [M]. 北京：电子工业出版社, 2002.
[16] 杨义先, 等.网络信息安全与保密 [M]. 北京：北京邮电大学出版社, 1999.
[17] 冯登国, 卿斯汉. 信息安全—核心理论与实践 [M]. 北京：国防工业出版社, 2000.
[18] Yang T, Chua L O. Impulsive stabilization for control and synchronization of chaotic systems [J]. **IEEE Trans. Circuits Syst. I,** 1997, 44(10): 976-988.
[19] Fridrich J. Symmetric ciphers based on two-dimensional chaotic maps [J]. **Int. J. Bifur. Chaos,** 1998, 8(6): 1259-1284.
[20] 丘水生, 陈艳峰, 等. 混沌保密通信的若干问题及混沌加密新方案 [J]. 华南理工大学学报, 2002, 30(11): 75-80.

作者简介：丘水生（1939-），男，广东平远人，华南理工大学教授，博士生导师，主要研究方向为非线性系统理论、混沌保密通信和功率电子学；陈艳峰（1970-），女，湖南永兴人，华南理工大学副研究员，博士，主要研究方向为非线性系统理论与混沌及功率电子学。

# A novel scheme of chaotic encryption system

QIU Shui-sheng,　CHEN Yan-feng,　WU Ming,
MA Zai-guang,　LONG Min,　Liu Xiong-ying
( College of Electronic & Information, South China Univ. of Tech., Guangzhou 510640, China )

**Abstract:** In this paper, the unpredictability of chaos is discussed, the method of producing chaotic signals is explored and chaotic encryption is compared with conventional encryption. Then a novel scheme of cascading chaotic stage and conventional encryption stage is proposed. The new scheme makes use of the unpredictability of chaotic systems. It is shown that the combination of chaotic encryption and conventional encryption is important for raising the security of cryptosystems.
**Key words:** circuits and systems; a novel scheme of cryptosystems; chaotic secure communication; chaotic cryptography

---

(续第 97 页) ( *from page* 97 )

# Study on UWB pulse design algorithm

ZOU Wei-xia[1],　DAI Wei-wei[1],　ZHAO Li-xin[1],　ZHOU Zheng[1],　ZHAO Chuan-hua[2]
( 1. Wireless Network Lab, Beijing University of Posts and Telecommunications, Beijing 100876, China;
2. Department of Chemistry and Chemical Engineering, Taishan Medical Institute, Taian 271000, China )

**Abstract:** Based on the characteristics of Rayleigh monopulse a novel algorithm to design UWB pulse is presented. It is not only simple but also applicable to the spectral mask of all countries. Theoretical analysis shows this pulse outperforms significantly the widely adopted Gaussian pulse in ultra-wideband impulse radio.
**Key words:** Ultra-Wideband impulse radio (UWB-IR); Rayleigh monopulse; power spectral density