物理真随机码发生器随机性分析*

魏正军 廖常俊 王金东** 郭健平 王发强 刘颂豪
(华南师范大学信息光电子科技学院光子信息技术实验室，广州 510631)

摘 要 对物理随机码发生器的物理参量与其产生的随机码序列的随机性关系进行了分析．根据量子保密通信对随机码序列的随机性的要求，分析了常见的随机码发生器产生的随机码的随机性，给出了利用随机高斯噪音经比较器产生随机码的随机码发生器的随机性公式．

关键词 量子保密通信；真随机码；信息熵；相关系数
中图分类号 TN918 **文献标识码** A

0 引言

随着全球信息化的发展，信息的安全问题已经成为世界各国重点研究的课题．量子保密通信系统通过两个方面的措施，为信息的传递提供绝对的安全性：1)采用物理的方法，利用量子力学的海森伯不确定性原理，建立不可窃听的量子信道，为密钥的传送提供绝对安全的通道[2]．2)数学上已经证明，一次一密系统是绝对安全的，不可破译的密码[2]．一次一密系统所需要的密钥的熵等于相应明文的熵，而且密钥只用一次．因此，需要的密钥量是巨大的，从而产生巨大的通信流量，密钥传送的安全问题，成为信息安全的重要问题．采用一次一密的加密方式，保证密文绝对不可破译．即，量子保密通信的绝对安全性由两个方面保证，防窃听的信道和永不重复的密码本—真随机码序列．本文主要讨论永不重复的密码本—真随机码序列的产生问题．

1 产生随机码的方法

1.1 数学方法

数学上常用的产生随机数的方法有：RAND 表产生伪随机数序列、线性同余发生器产生伪随机数序列、反馈移位寄存器产生伪随机数序列、伪随机数发生器 ANSI X9.17 等等．这些用数学方法产生的伪随机数序列只由算法和种子决定，一旦算法和种子确定以后，序列中的每一位的值都是确定的，因此，这种方法产生的随机数序列被称为伪随机数，它的信息熵为零，不能用于量子保密系统[3]．

2.2 物理方法

物理上的产生随机码的方法是把自然界的模拟随机信号通过非线性变换系统，得到离散二进制随机码．其原理如图 1.

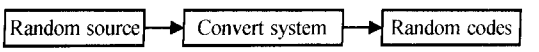


图 1 物理真随机码发生器原理
Fig. 1 Schematic of true random number generator

常见的随机信号源有：

1)选取真实世界的自然噪音．自然界存在丰富的随机现象，可以利用各种噪音信号本身的随机性来获得真随机码[4,5]．

2)量子随机事件．被囚禁的离子产生的共振荧光辐射，其光子间隙时间是随机分布的，光子通过光学分束器的随机性等等[6,7]．

非线性变换系统，一般都采用单阈值的比较器甄别方案．

2 量子密钥分发过程对随机码的要求

在实际量子密钥分发系统中，收发双方 Alice 和 Bob 需要使用随机码来随机制备和随机检测单光子的量子态．量子密码序列是从随机码序列中提取出来的[8~12]，为使探测结果不相关，此随机序列必须是真随机的．实现一次一密，随机码也必须是永不重复的．即量子密码的产生和使用都要求采用真随机码．因此对随机码的要求是[13]：

1)由一次一密的原理，密钥的信息熵必须大于等于明文的信息熵，所以，随机码的信息熵越大越好．熵的计算公式为

$$H(x)=-\sum_{i=1}^{n}p(x_i)\log_2 p(x_i) \tag{1}$$

式中 $p(x_i)$ 为随机码中 0 和 1 的概率．当 0 和 1 等概率地出现时，随机码的熵达到最大，有最大的不确定性．

2)随机码的各位必须统计独立，以避免被窃听者根据密码通信双方在公开信道上公布的部分结果，推出未公布作为密钥的部分．

3 随机码发生器输出的随机性分析

长期以来，对于物理随机码发生器的物理参量

*国家 973 科研计划(2001CB309300)、广东省科研基金(2003A1030405)和广州市科研基金(1999Z03501)资助项目
** Tel：020-85213862 Email：jindongw@126.com
收稿日期：2005-11-22

与其产生随机码序列的随机性的关系，缺乏定量的理论分析．对常见的噪音而言(如电压、电流等大多数物理量的噪音)，都遵从正态分布或高斯分布．本文就以采用随机高斯噪音作为随机源，以单阈值的幅度甄别器为变换系统的随机码发生器为例，分析其产生的随机码的随机性．设随机码发生器当随机高斯噪音的幅度低于甄别电平时，输出为 0，高于甄别电平时，输出为 1.

随机高斯过程的几率密度函数表示为[14]

$$P(x)=\frac{1}{\sqrt{2\pi}\sigma}\exp\{-[x-m_x(t)]^2/2\sigma^2\} \tag{2}$$

式中 σ 为该物理量的方差，$m_x(t)$ 为该物理量的数学期望．

3.1　信息熵分析

对于单阈值随机码发生器，随机信号源通过比较器转换为随机码，这是随机过程的一种典型的阈交问题．输出为 0 和 1 的概率分别为

$$p(x=0)=\int_{-\infty}^{V_a}\frac{1}{\sqrt{2\pi}\sigma}\exp\{-[x-m_x(t)]^2/2\sigma^2\}\mathrm{d}x \tag{3}$$

$$p(x=1)=\int_{V_a}^{-\infty}\frac{1}{\sqrt{2\pi}\sigma}\exp\{-[x-m_xt]^2/2\sigma^2\}\mathrm{d}x \tag{4}$$

当阈值

$$V_a=m_x(t) \tag{5}$$

时，设

$$y=x-m_x(t) \tag{6}$$

则

$$p(x=0)=\int_{-\infty}^{V_a}\frac{1}{\sqrt{2\pi}\sigma}\exp\{-[x-m_x(t)]^2/2\sigma^2\}\mathrm{d}x=\int_{-\infty}^{0}\frac{1}{\sqrt{2\pi}\sigma}\exp\{-y^2/2\sigma^2\}\mathrm{d}y=\frac{1}{2} \tag{7}$$

$$p(x=1)=\int_{V_a}^{+\infty}\frac{1}{\sqrt{2\pi}\sigma}\exp\{-[x-m_x(t)]^2/2\sigma^2\}\mathrm{d}x=\int_{0}^{+\infty}\frac{1}{\sqrt{2\pi}\sigma}\exp\{-y^2/2\sigma^2\}\mathrm{d}y=\frac{1}{2} \tag{8}$$

此时输出的随机码中 0 和 1 等概率出现，随机高斯噪音在比较器门限电压的上、下等概率地分布，信息熵最大．所以比较器的参考电压必须等于随机噪音源信号的数学期望 $m_x(t)$.

虽然对于平稳高斯随机过程，$m_x(t)$ 是不随时间变化的，但平稳随机过程只是短时间内的理想近似，在长期工作的情况下，其数学期望 $m_x(t)$ 随时间的改变是不能忽略的．由于 $m_x(t)$ 是随时间变化的变量，要获得最大的信息熵，必须实时地保持门限电压总是等于随机高斯噪音的数学期望．

3.2　随机码的自相关系数

随机码的自相关系数由物理随机源的随机性和变换系统的系统传递函数共同决定的．

对于单门限甄别电路，它利用阈交事件产生随机码输出，输出的随机码的自相关函数为

$$R_x(\tau)=E[x(t_1)x(t_2)]=1\cdot1\cdot p[x(t_2)=1|x(t_1)=1]+0\cdot1\cdot p[x(t_2)=1|x(t_1)=0]+1\cdot0\cdot p[x(t_2)=0|x(t_1)=1]+0\cdot0\cdot p[x(t_2)=0|x(t_1)=0]=p[x(t_2)=|x(t_1)=1] \tag{9}$$

即自相关函数为随机码序列在 t_1 和 t_2 这两个采样点上同时取 1 的概率．若在时间间隔 $\tau=t_2-t_1$ 内，发生阈交的次数为偶数，则 $x(t_1)$ 和 $x(t_2)$ 同取 1 或者 0. 对于平稳随机过程，$x(t_1)$ 和 $x(t_2)$ 同取 1 或者 0 的概率相等，为

$$p[x(t_2)=1|x(t_1)=1]=p[x(t_2)=0|x(t_1)=0]=\frac{1}{2}\sum_{0}^{2n}p_k[N(\tau)] \tag{10}$$

式中 $p_k[\bar{N}(\tau)]$ 为在 $\tau=t_2-t_1$ 时间内，阈交事件发生 k 次的概率．

在单位时间内正阈交的平均次数[15]

$$\bar{N}=\int_0^{\infty}\dot{x}p_2(x_0,\dot{x})\mathrm{d}\dot{x} \tag{11}$$

对于平稳高斯随机过程

$$\bar{N}=\frac{\sigma_{\dot{x}}}{2\pi\sigma}\exp\left[-\frac{(x_0-m_x)^2}{2\sigma^2}\right] \tag{12}$$

给定的时间间隔 τ 内的正阈交发生 k 次的概率 $p_k[\bar{N}(\tau)]$，如果在 τ 时间内，发生的次数不是很高时，近似服从柏松分布

$$p_k[\bar{N}(\tau)]=\frac{[\bar{N}\tau]^k}{k!}\exp[-\bar{N}\tau] \tag{13}$$

对于平稳高斯随机过程，单位时间内正阈交的平均次数等于负阈交的平均次数．所以单位时间总的阈交的平均次数为 $2\bar{N}$.

对于平稳随机过程在任一时间间隔 $\tau=|t_i-t_1|$ 内，相关系数与时刻无关，仅是时间间隔的函数．输出的随机码的相关函数为

$$R_x(\tau)=E[x(t_1)x(t_2)]=\frac{1}{2}\mathrm{e}^{-2\bar{N}\tau}\left[1+\frac{(2\bar{N}\tau)^2}{2!}+\frac{(2\bar{N}\tau)^4}{4!}\cdots\cdots\right]=\frac{1}{4}+\frac{1}{4}\mathrm{e}^{-4\bar{N}\tau} \tag{14}$$

其归一化自相关函数为

$$r_x(\tau)=\mathrm{e}^{-4\bar{N}\tau} \tag{15}$$

对于平稳高斯过程，当阈值 $V_a=m_x$ 时，有

$$\bar{N}=f_0 \tag{16}$$

式中，f_0 为高斯白噪音的平均频率．所以有

$$r_x(\tau)=\exp[-4f_0\tau] \tag{17}$$

由式(17)可知，输出的随机码的归一化自相关

函数是随机码的周期 τ 和高斯白噪音的平均频率 f_0 的函数，如图 2.

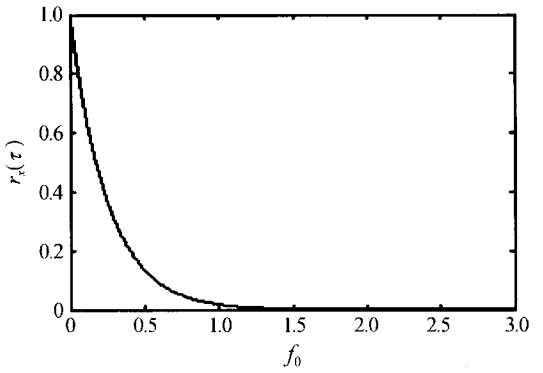


图 2 随机码的归一化自相关函数曲线

Fig. 2 The autocorrelation function with τ

工程应用当中，当τ大到一定程度时，如果 $r_x(\tau)$已经很小，则可近似认为 $X(t)$和 $X(t+\tau)$之间已不存在任何关联，统计独立．这里引入相关时间 τ_0．当 $\tau>\tau_0$ 时，则可以认为 $X(t)$和 $X(t+\tau)$之间已不相关．τ_0 的定义为

$$|r_x(\tau_0)|\leqslant 0.05 \tag{18}$$

从上面的分析可知，当单门限随机码发生器的取样时间大于 τ_0，即 $f_0\cdot\tau\geqslant 0.749$ 时，可以认为输出的随机二进制序列的各位之间是不相关的，即输出为真随机码．但是 τ_0 过大时，限制了随机码的产生速率，需要通过增大随机噪音信号源的带宽来解决，这就对随机噪音信号源提出了更高的要求．

4 结论

本文根据量子保密通信对随机码序列的随机性的要求，以随机高斯噪音经比较器产生随机码的随机码发生器为例，分析了常见的随机码发生器产生的随机码的随机性，给出了随机源和变换系统对随机码发生器输出的随机序列的信息熵和自相关系数的关系式，有助于量子保密通信安全性的研究工作．

参考文献

1 Paul D T. A quantum key distribution channel based on optical fibre. *Journal of Modern Optics*, 1994, **41**(12): 2425～2433

2 杨义先，林须端. 编码密码学. 北京：人民邮电出版社，1992. 53～68
Yang X Y, Lin Lin X D. Code and Cryptography. Beijing: Posts & Telecom Press, 1992. 53～68

3 邓乐，毛敏，张涌，等. 应用伪随机序列的量子密码术. 量子光学学报，1999，**5**(3)：172～176
Deng L, Mao M, Zhang Y, *et al*. *Acta Sinica Quantum Optica*, 1999, **5**(3): 172～176

4 辛茜，曾晓洋，张国权，等. 基于电阻热噪音的真随机数发生器设计. 微电子学与计算机，2004，**21**(7)：143～146
Xin Q, Zeng X Y, Zhang G Q, *et al*. *Microelectronics & Computer*, 2004, **21**(7): 143～146

5 孙建伟，张胜利，王绍伟. 用白噪音源实现高速真随机码. 电子学报，2003，**31**(8)：1255～1256
Sun J W, Zhang S L, Wang S W. *Acta Electronica Sinica*, 2003, **31**(8): 1255～1256

6 廖静，梁创，魏亚军，等. 基于光量子的真随机源. 物理学报，2001，**50**(3)：467～472
Liao J, Liang C, Wei Y J, *et al*. *Acta Physica Sinica*, 2001, **50**(3): 467～472

7 冯明明，秦小林，周春源，等. 偏振光量子随机源. 物理学报，2003，**52**(1)：72～75
Feng M M, Qing X L, Zhou C Y, *et al*. *Acta Physica Sinica*, 2003, **52**(1): 72～76

8 Bennett C H, Brassard G, Bessette F, *et al*. Quantum cryptography: Public2key distribution and coin tossing. In: Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, 1984. 175～179

9 Bennett C H, Bessette F, Brassard G, *et al*. Experimental quantum cryptography. *Journal of Cryptology*, 1992, **5**(1): 3～28

10 Ekert A K. Quantum cryptography based on Bell′s theorem. *Phys Rev Lett*, 1991, **7**(6): 661～663

11 刘景锋，梁瑞生，唐志列，等. 基于 BB84 协议的实际 QKD 系统的窃听问题研究. 光子学报，2004，**33**(11)：1356～1359
Liu J F, Liang R S, Tang Z L, *et al*. *Acta Photonica Sinica*, 2004, **33**(11): 1356～1359

12 陈志新，唐志列，魏正军，等. QKD 系统在 Breidbart 基窃听下 BB84 协议的信息量研究. 光子学报，2004，**33**(12)：1470～1472
Cheng Z X, Tang Z L, Wei Z J, *et al*. *Acta Photonica Sinica*, 2004, **33**(12): 470～1472

13 Rarity J G. Quantum random-number generation and key sharing. *Journal of Modern Optics*, 1994, **41**(12): 2435～2444

14 纽兰 D E. 随机振动与谱分析概论. 北京：机械工业出版社，1980. 87～100
Newland D E. An introduction to random Vibratuons and Spectral analysis. Beijing: China Machine Press, 1980. 87～100

15 章潜五. 随机信号分析. 西安：西北电讯工程学院出版社，1986. 140～147
Zhang Q W. Stochastic Signal Analysis. Xi′an: Xidian University Press, 1986. 140～147

Randomicity of Physical Random Number Generator

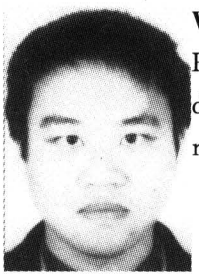
Wei Zhengjun, Liao Changjun, Wang Jindong, Guo Jianping, Wang Faqiang, Liu Songhao

Lab of Photonic Information Technology, School for Information and Optoelectronic Science and Engineering, South China Normal University, Guangzhou 510631

Received date: 2005-11-22

Abstract The absolute security of quantum cryptography system was guaranteed by two aspects: no eavesdropping channel and no repetition true random codes. The randomicity of physical random number generator based on Guass noise was discussed. The relation of its correlation coefficient and entropy with the physical parameter were calculated and how to get the best performance was discussed. It is useful for developing the true random number generator used in the quantum cryptography systems.

Keywords Quantum cryptography systems; True random number; Correlation coefficient; Entropy



Wei Zhengjun was born in 1977. He received his Bachelor's degree in the Department of Physics of South China Normal University in 2004. He is carrying out his master Master's degree research on the practical technique of quantum cryptography system. His current research is on the single photon detection.