Application of the Generation of Gaussian Random Number in Quantum Cryptography

WANG Lingzhi[1], WU Yichun[1], WANG Yong[2]

1. College of Physics and Information Engineering, Zhangzhou Normal University, Zhangzhou, China

2. Institute of Plasma Physics, Chinese Academy of Sciences, Hefei, China

e-mail: wanglingzhiwlz@163.com, ycw@ipp.ac.cn, wayong@ipp.ac.cn

Abstract: With the development of the information time, the security of the information system is more and more important. Having well known on the study of the current situation about quantum cryptographic key, Reverse Reconciliation Gaussian-moduled quantum key distributed Protocol (Abr. RR) is concerned in this paper. A design scheme of cryptogram transmission system based on FPGA is presented, which is used to implement the simulation of the Quantum Key Distributed. To simulate the preparation of the secret-key, a Gaussian random number generator in FPGA is designed, which based on the analysis of Ziggurat algorithm. The period length of generated Gaussian random secret-key is longer than 2^{88}, and its precision is high (achieve 26 fractional bits). Furthermore, the generated Gaussian random number has passed the normal test. It provides a new method to prove the correction of RR protocol and study of QKD.

Keywords: QKD; Reverse Reconciliation; FPGA; Gaussian random number

量子密钥分发协议中高斯随机数发生器的设计

王灵芝[1]，吴一纯[1]，王勇[2]

1.漳州师范学院物理与电子信息工程系，漳州，中国，363000

2.中科院等离子体物理研究所，合肥，中国，230031

e-mail: wanglingzhiwlz@163.com, ycw@ipp.ac.cn, wayong@ipp.ac.cn

【摘　要】随着社会信息化的不断推进，人们对于建立真正安全的信息保密系统的愿望越来越迫切。在深入调查量子密码研究现状的基础上，本文针对 Reverse Reconciliation Gauss-moduled 量子密钥分发协议(简称 RR 协议)进行了分析与研究，提出了基于 FPGA 的密钥传输系统的设计方案，用于模拟高斯密钥的分发过程。为了模拟密钥的制备，在分析 Ziggurat 算法的基础上完成了高斯随机数发生器的 FPGA 实现。由此产生的高斯密钥周期长(大于 2^{88})，精度高(小数部分等于 26b)，并且通过了正态分布检验，为验证 RR 协议的正确性乃至量子加密的研究提供一个新的手段。

【关键词】量子密钥分发；Reverse Reconciliation；FPGA；高斯随机数

1 引言

量子密码术是量子物理学与密码学相结合的一门新兴学科，它成功解决了经典密码学中单靠数学无法解决的问题，从而建立了真正安全的信息保密系统。目前对该领域研究最多的是关于量子密钥分发的问题（Quantum Key Distributed，简称 QKD），一些技术已经从理论走向实用化。例如单光子的传输协议 BB84：通信双方由一个量子通道和一个经典的公共通道连接起来。单光子携带信息通过量子通道(如光纤)来传递密钥。经典的公共通道是常规的通讯信道(如电话或因特网等等)，用于原始密钥的确认和比较。但两个主要问题限制了其实用性：首先是没有合适的单光子光源；其次是单光子探测器的效率和速度跟不上。

近年来，国外一些研究小组已经开始了连续变量密码术的研究[1,2]。与单光子传输不同的是，连续变量的量子密码术以光束（如图 1 所示）作为信息载体，使其具有高效率和高比特率等优点，并且在很多方面与目前成熟的光通信技术兼容，是量子密码术今后发展的方向。本文讨论的正是基于连续变量的 Reverse Reconciliation Gauss-moduled QKD 协议（简称 RR 协议）。

随着量子密码的实用化进程的推进，减少设备体积以及与其它设备集成是必然趋势，如果能将量子密码系

基金项目：国家自然科学基金项目（No.10675128）资助

978-1-935068-06-8 © 2009 SciRes.

统集成在一个微小的芯片上是最理想不过的。此外，昂贵的实验设备以及苛刻的实验环境都限制了对量子密码的深入分析与研究，通过计算机对 QKD 协议进行仿真将为量子密码系统的研究提供一种新的手段。

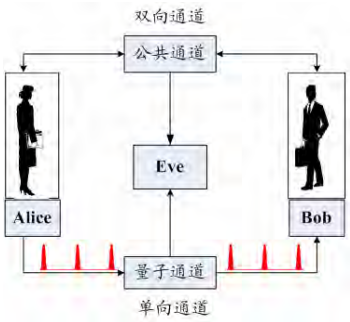

Figure 1. Schematic diagram of quantum cryptography with continuous variable

图 1. 基于连续变量的量子密码术示意图

2 RR 协议的分析与讨论

2000 年，Cerf[3]提出了应用单模正交压缩相干态光场作为信息载体，通过调制光场的振幅和相位来完成信息编码的方案。此后，G.Van Assche 提出了 Reverse Reconciliation (RR) 的高斯密钥分发算法[4,5]。在 RR 协议中，Alice 和 Bob 也是通过一个量子通道和一个经典的公共通道连接起来，与 BB84 不同的是在量子通道上传送的是光场压缩态而不是单光子偏振态。协议包括了量子密钥制备、窃听者检测、数据纠错、隐私放大等过程。

由信息论可知：一个连续的信号当其方差(平均功率)受限，概率密度函数在呈高斯分布时信源熵最大[6]。因此利用高斯信号来调制密钥信息可获得最大信息量。

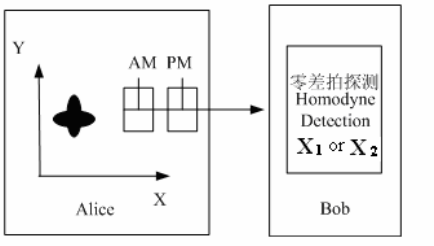

Figure 2. Schematic diagram of quantum cryptography with quadrature squeezed state light

图 2. 用正交压缩光实现量子密码术实验示意图

在密钥的制备上，RR 协议规定：Alice 一方将连续相干光进行相位和幅度调制成光脉冲，发送具有高斯分布的密钥信息，在 Bob 一方进行零差拍的探测。如图 2 所示，AM 为幅度调制器，PM 为相位调制器。

当 $|X_1\rangle$ 被选时，Alice 把待传送的信息 x_1 以 AM 方式调制到 $|X_1\rangle$ 之上，经压缩调制后的载波振幅分量满足高斯分布 $N(x_1,\sigma_1)$，信息 x_1 满足 $N(0,\sum_1)$ 分布。载波表示为

$N(x_1,\sigma_1)\times N(0,¼\sigma_2)$，

其中 $\sigma_1 < 1/2$。

Alice 随机选择 $|X_1\rangle$ 或 $|X_2\rangle$ 作为经典信息的载体，由于 $|X_1\rangle$、$|X_2\rangle$ 是非对易的相干态，二者之间满足测不准关系 $\Delta X_1 \Delta X_2 \geq ¼$。

当 $|X_2\rangle$ 被选择时，Alice 把待传送的信息 x_2 以 PM 方式调制到 $|X_2\rangle$ 上；经压缩调制后的载波相位分量满足高斯分布 $N(x_2,\sigma_2)$，信息 x_2 满足 $N(0,\sum_2)$ 分布。则载波为 $N(0,¼\sigma_1)\times N(x_2,\sigma_2)$，其中 $\sigma_2 < 1/2$。

然后，Alice 把调制后的量子态 $|X_1\rangle$ 或 $|X_2\rangle$ 发送给 Bob，Bob 随机地选择正交振幅分量或正交相位分量进行测量接收。在等式

$\Sigma_1^{\,2}+\sigma_1^{\,2}=1/16\sigma_2^2$、$\Sigma_2^{\,2}+\sigma_2^{\,2}=1/16\sigma_1^2$

成立的条件下，若 Alice 选择 AM 发送，Bob 选择 AM 来测量时，那么在不考虑信道噪音的情况下，经过零差拍探测到的结果满足方差为 $\sum_1^{\,2}+\sigma_1^{\,2}$ 的高斯分布；若 Bob 选择 PM 来测量，根据测不准原理，结果满足方差为 $1/16\sigma_2^2$ 的高斯分布；反之亦然。因此经过高斯调制后的相干态具有相同的方差使得窃听者不能区别。在量子通道密钥发送完毕之后，双方利用特定的 Sliced 算法将连续的数据转换成普通的二进制密钥。此后 Bob 在公开信道上告诉 Alice 他每次选择测量是振幅分量还是相位分量(但不公布测量结果)。为了检测窃听者的存在，双方可公开一部分比特进行比较。如果误码率在容忍的范围内，则剩余的比特可作为安全的密钥使用。否则，可判定有窃听者存在。因此即便在线路损失的情况下，Alice 也比潜在窃听者 Eve 具有优势，此外协议还可以降低随机损失。

3 基于 FPGA 的 RR 协议的仿真系统的设计

Gottesman-Knill[7]定理指出对于仅包括量子态制备和量子态测量的量子密钥分配协议可以通过经典的

计算机有效仿真。通过对 RR 协议的分析可知，在密钥制备的过程中，必须产生高斯信号源对其进行调制，而且密钥信号也是满足高斯分布的随机数，因此我们选择用 FPGA 产生满足高斯分布的随机数来模拟这一过程。Alice 和 Bob 在公共信道上的讨论涉及到对离散的二进制信息的处理过程，也可通过经典的计算机进行有效仿真。因此对 RR 协议的仿真系统的构建可以 FPGA 和 PC 机共同实现，从而验证协议的安全性以及各种攻击策略的有效性，为量子密钥分配协议的研究提供一种新手段。

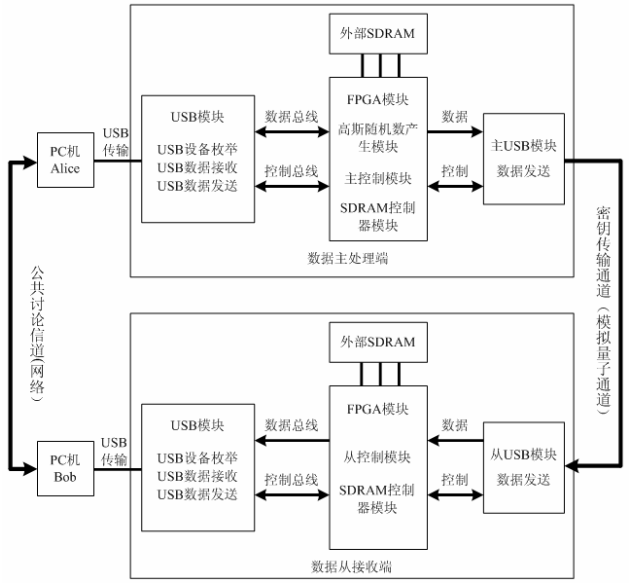

Figure 3. Hardware block diagram of quantum cryptography transmission system base on FPGA

图 3. 基于 FPGA 的 RR 量子密码传输系统的硬件框图

图 3 为基于 FPGA 的密码传输系统的硬件框图。此系统主要由两大部分组成，分别模拟数据的发送方（Alice）和接收方(Bob) 通过量子通道发送高斯密钥信息以及通过公共信道讨论的过程。数据主处理端由 FPGA 产生一系列的高斯随机数通过 USB 模块回传给 Alice 一方的 PC 机。同时这些数据通过主 USB 模块发送到从处理端，最后传给 Bob 的 PC 机，完成对量子传输通道的模拟。此后，Alice 与 Bob 通过公共信道（Internet）进行讨论，完成对 RR 协议的计算机模拟，最终获得一致的密钥信息。

如图 4，FPGA 内部电路主要由 4 个部分构成：高斯随机数发生器(GNRG)、FIFO、主控制器（Maincntl）、SDRAM 控制器(SDRAMcntl)；高斯随机数产生模块产生密钥信息；SDRAM 控制器模块实现对外部 SDRAM 的读写[8]；控制器模块产生地址信号和控制信号。系统首先将产生的密钥信息写入 SDRAM，直到存满。之后再通过控制器模块将 SDRAM 数据读出送给 USB 模块，最终传给双方的 PC 机。从而大大提高了系统的传输速度。

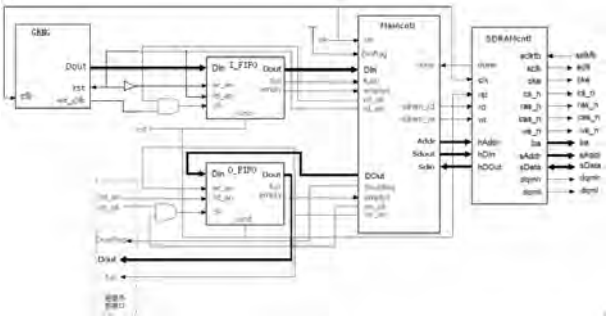

Figure 4. Structure diagram of internal circuit in FPGA

图 4. FPGA 内部电路结构框图

4 基于 FPGA 的高斯随机数发生器

在 RR 协议中，原始密钥是满足高斯分布的一连串的随机数，可以通过硬件来模拟其制备的过程。高斯分布是自然界中最常见的一种信号分布形式。高斯随机数产生器(GNRG)广泛应用于数字建模、通信系统、工业控制中。

目前已有的高斯随机数产生算法主要包括：Danger 算法[9]、Byungyang Ahn[10]算法等。本文基于 Ziggurat 算法[11]来产生随机的高斯变量：

如图 5 所示：假设 C 代表曲线 $y=f(x)=e^{-x^2/2}$ 与 X 轴包围的区域，面积为 1。用 n 个矩形和一个尾部叠加来近似曲线 C，最后一个矩形与尾部的面积之和与其余的矩形的面积相等，用 v 表示每个矩形面积，$v=1/n$。把矩形包围的区域用 Z 来表示。在 Z 中，随机点 (x,y) 满足均匀分布，算法接受所有落入 C 区域的随机点。当 n 足够大时，Z 的概率密度 $Z(x)$ 将十分接近正态分布。通过 Ziggurat 算法分析可知，对矩形区的计算涉及到均匀分布随机数的产生、乘法逻辑、数组逻辑等等，这些在 FPGA 中都可以实现，而对楔形区、尾部的实现涉及到对数函数与指数函数的运算，用硬件实现比较困难。并且当取 n=1024 时，落入矩形区的比率为 99.84%。已经能够满足要求，因此在本节中只考虑矩形区的实现。

978-1-935068-06-8 © 2009 SciRes.

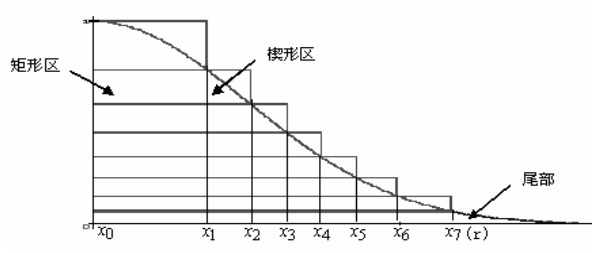

Figure 5. Schematic diagram of Ziggurat algorithm

图 5. Ziggurat 算法示意图

图 6 为高斯随机数发生器模块结构图，ROM 存有 1024 个 16bit 矩形端点 $x_i[1024]$；URNG 均匀随机数产生模块产生在[0,1]上均匀分布的 32 位随机数，取出其低 10 位作为 ROM 的地址信号 addr 进行寻址，得到矩形端点 $x[addr]$。取 URNG 高 16 位数据经过延时电路与 $x[addr]$ 一起送入 16×16bit 的乘法器中，最终输出宽度为 32bit 宽度的数据。乘法器采用了 3 级流水，数据产生的速度主要由乘法器决定。VHDL 硬件描述语言编写各个模块。

其中 URNG 模块采用 Tausworthe 随机数产生器构成，它结合了 3 个 LFSR 能够在消耗不多硬件资源的前提下满足要求，来提高统计性能，随机序列的周期长度可以达到 2^{88} [11]。

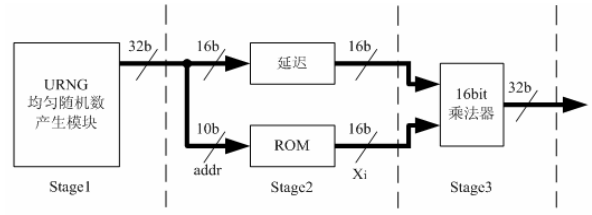

Figure 6. Structure diagram of Gaussian random number generator module

图 6. 高斯随机数发生器模块结构图

5 实验结果与数据分析

图 7 是高斯随机数发生器的 modelsim 仿真时序图，clk 为系统的主时钟，reset 为复位信号，信号 xi 为 ROM 存储器的输出结果，jout 为 URNG 模块经过 D 触发器的输出信号。Mutdata 是 16X16bit 乘法器的输出，xi 与 jout 信号的高 3 位表示整数、低 13 位表示小数。最终产生的高斯随机数小数部分等于 26b。仿真波形时序很好地符合了设计要求，从而验证了电路的正确性。

利用 MATLAB 软件对仿真数据进行正态分布统计检验。首先将 32 位的二进制数据转换成实数，其中高 6 位代表整数、低 26 位代表小数。利用 MATLAB 统计学工具箱中正态分布检验两个工具：btest 检验算法与 normfit 检验算法。

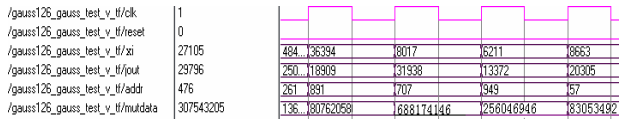

Figure 7. Simulating timing diagram of Gaussian random number generator

图 7. 高斯随机数产生器电路的仿真时序图

设定 α =0.05， P_{ci} =0.95。结果表明数据均值为 μ =-0.0069，方差 σ^2 =1.0084，通过了 Jbtest 检验和 normfit 检验。产生的高斯密钥满足了标准正态分布 N(0,1)。

6 结论

在对基于连续变量的 Reverse Reconciliation Gauss-moduled QKD 协议分析的基础之上，本文提出了基于 FPGA 的 RR 协议的仿真系统的设计方案。利用 FPGA 产生高斯随机数并在 RR 协议中应用的，由此产生的高斯密钥周期长，精度高，并且通过了正态分布检验。为验证 RR 协议的正确性乃至量子加密提供指导和参考。

References (参考文献)

[1] Ralph T C. Cobntious variable quantum cryptography [J]. Phys. Rev. A, 2000, 61, P010303.
[2] Hillery M. Quantum cryptography with squeezed states [J]. Phys. Rev. A, 2000, 61, P022309.
[3] Cerf N, Levy M, Van Assche G. Quantum distribution of Gaussian keys using squeezeed states [J]. Phys. Rev. A, 2001, 63, P052311.
[4] Grosshans F, Van Assche G, Wenger J. Reverse reconciliation protocols for quantum cryptography with continuous variables [J]. Nature, 2003, 421, P238.
[5] Van Assche G, Cardinal J, Nicolas J Cerf. Reconciliation of a quantum distributed Gaussian key [J]. IEEE, Feb. 2004, 50(2), P394-400.
[6] Tao Chunzhan, Tao Chunkuang. Optical Information Theory [M]. Beijing: Science Press, 1999, P23-24(Ch).
陶纯堪,陶纯匡.光学信息论[M].北京:科学出版社,1999,P23-24.
[7] Nielsen M A, Chuang I L. Quantum Computation and Quantum Information. Cambridge [M]. U.K. Cambridge University Press, 2000, P64.