基于量子通信的数字档案安全传输技术研究与探索

向 禹 吴湘华 郭 迎
中南大学 长沙 410083

摘 要：数字档案馆，特别是档案在线服务平台的建设给档案用户带来了便捷，档案在提升远程服务能力的同时，在数据传输过程中也带来了安全隐患。文章基于量子通信技术，对数字档案安全传输技术进行了研究与探索，努力构建档案安全体系。

关键词：档案安全；数据传输；量子通信；量子密码

0 引言

随着档案信息化的发展，特别是数字档案馆的建设，提升了档案远程服务能力，为用户带来更为便捷的体验，为人们提供更为贴心的档案服务。以中南大学档案馆为例，建成的数字档案馆公共服务平台已实现在线办理档案业务，在线授权阅读数字档案。但由于档案的隐私性、凭证性、唯一性，远程传输数字档案却带来了安全隐患。

通过中国知网中输入检索式“TI=档案 * 安全 *(数据 + 电子)”，得到检索结果 304 条；而输入检索式“TI= 档案 * 安全 * 传输”，得到结果仅 1 篇。数字档案安全研究主要集中在数据安全存储、数字档案安全管理、档案管理系统的权限控制与设计、服务器安全管理等方面，而数字档案传输过程中的安全问题研究仍然少有人触及。如何解决档案便捷服务与数据安全的巨大矛盾是档案信息化建设面临的现实问题，相比数据存储、服务器及系统安全来说，数字档案传输的安全性更容易被人们忽视，技术实现难度也更大。

1 量子密码通信技术研究现状

IBM 公司科学家 C. H. Bennett 和加拿大 Montréal 大学密码学家 G. Brassard 于 1984 年提出第一个量子密码分发协议 BB84 协议[1]。在随后的数年里，国际上多名科学家已相继证明了量子密码的无条件安全性[2-6]。在实验方面，量子密码通信也在不断发展。由于离散变量量子密码通信的量子密钥分发协议的不安全性导致数据容易被窃听[7]，以及效率较低等因素，澳大利亚学者 T. C. Ralph 在 1999 年从实验角度首先提出了连续变量量子密钥分发的概念。D. Gottesman 和 J. Preskill 提出了一种利用压缩态实现的量子密钥分发方案，并利用连续变量纠错码的方法证明了该方案的安全性，第一次证明了连续变量量子密码的安全性[8]。基于光纤传输的首个连续变量量子密钥分发（QKD）方案是在 2005 年 11 月由 Philippe Grangier 小组提出的[9]，为实现连续变量量子密钥分发的光纤网络化做了非常好的尝试。由于连续变量量子秘密共享技术可应用于多方量子密钥分配，连续变量量子秘密共享技术也受到了人们的关注。

我国在连续变量 QKD 方面开展研究的单位也有很多，也取得了一些成果，与国际上相比还有些差距，但是在实验研究方面，特别是系统研制方面则相差不大。我国低速连续变量量子密码样机系统的部分参数达到了国际先进水平，部分技术指标达到了国际领先水平；高速连续变量量子密钥分配技术也有了一些研究。

国家档案局科技计划项目《基于连续变量量子密码通信的档案数据安全传输技术研究》2014-X-69，阶段性成果。

2 基于连续变量 QKD 档案传输模型设计

采用普通数据传输技术的数字档案，容易被截获而导致信息泄露，甚至发生泄密事件；因此，项目研究在数字档案传输过程中引入连续变量量子密码通信技术，开展数字档案安全传输实验和外场试验。为解决数字档案，特别是机密数字档案的传输问题进行了探索。

为实现数字档案的安全传输，根据数字档案的特点，必须研究长距离连续变量量子保密通信技术、高速平衡探测器技术、秘密协商算法、连续变量量子保密通信等有关数据传输安全的核心技术，将数字档案转换成量子信号，并进行技术加密，通过光纤传输，在远程接收端解码，最终获得数字档案。数字档案安全传输模型如图 1 所示。

在数字档案传输前，连续变量 QKD 给这些数据按照算法分配密钥 Key，并将数据转换成量子信息；携带 Key 的数字档案，通过光纤传输到远程端；在用户接收端，通过专用的接收设备对数据进行解析，若信息不变，且密钥准确，便还原成数字档案；在传输过程中，通过监控设备取样，用软件模块进行分析，使得整个传输过程可监控。数字档案安全传输模型中，还包括以下 5 个方面：

⑴ 设计连续变量 QKD 分配方案。结合现代光通信中的编码技术（特别是 4PSK 编码技术）和离散调制连续变量量子密码技术，研究适合在档案全文数据库与远程接收端之间通过光纤通信系统中高速运行的连续变量量子密码方案。

⑵ 过噪声的机理分析与抑制技术。在量子密码分配系统中，过噪声主要来自光源、信道、检测模块等几个部分，不同机制的过噪声需要采取不同的抑制技术。从系统整体上进一步抑制系统的过噪声，主要方法是参照传统光通信中的方式开展研究。针对系统中的主要模块，分析系统的过噪声机制，然后针对这些不同的过噪声机制，设计出相应的抑制算法或模块，提升系统的额稳定性和鲁棒性。

由于量子密钥分配系统中用于编码的相位、振幅等的幅度都很小，对外界的干扰比较敏感。如何抵抗这些环境干扰，使系统稳定呢？在传统的光通信中已经有一些现成的算法，但是这些算法不是很适合量子通信系统，本项目将在这些算法的基础上进行改进，从而实现系统的鲁棒性。

⑶ 基于 DSP 的平衡接收机技术。平衡接收机技术是连续变量量子信息处理实验实现中的核心技术之一。在参考现代光通信中的相干光通信技术的基础上，研究连续变量 QKD 中高速信号采集技术，由此预期可获得适合量子通信的基于 DSP 的平衡接收机核心技术。除高速采集技术外，研究检测模块的噪声抑制技术，设计出相应的电路模块。

⑷ 高速连续变量 QKD 系统。利用项目所研发的软件模块和电路驱动模块，在所提出的连续变量量子密钥分配方案的基础上，构建一个稳定的、安全的、高速的连续变量量子密钥分配模块。

⑸ 数字档案传输安全性监控技术。在已有低速连续变量 QKD 技术基础上，根据高速 QKD 系统的技术特点研制一套适合档案数据安全传输系统的安全性监控技术。核心技术是采用多节点监控，然后通过自行研制的软件完成综合分析，并给出结论。

量子密钥分配方案已经被证明具有无条件安全性，但是，对于一个量子密钥分配系统而言却并非如此，这里涉及一个理论安全性与实际安全性的问题。最近研究表明，多个方面的因素如光源、随机数、信道、软件模块、检测等部分都可能引入边信道，从而影响系统的安全性。项目将通过软件模块监控各个部分的参数来整体分析系统的实际安全性。课题组已经完成了低速下的 QKD 系统的安全性监控软件，项目将研究高速量子保密通信系统的安全性监控问题。

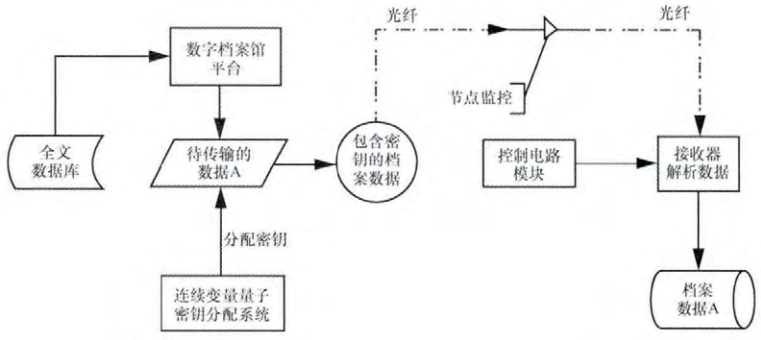

图 1 档案数据安全传输模型

3 数字档案传输系统研究

基于中南大学数字档案馆公共服务平台、全文数据库而进行的研究实验，已经基本解决系统本身的数据存储和管理方面的安全性问题。在档案数字传输过程中，要防范数据被窃听、截获或破坏，按照档案数据安全传输模型设计进行实践和研究。

3.1 数字档案传输方案设计

近年来，基于高斯调制的连续变量量子密码得到了充分的研究，但这种方式给后面的秘密协商带来了一定困难。考虑到离散变量量子密码中秘密协商的简便性，基于离散调制的连续变量量子密码自然成为人们考虑的问题。研究表明，这种方式同时具有离散变量和连续变量量子密码的特点，项目结合现代光通信中的编码技术，如 DPSK，4PSK，ASK 等编码技术，采用星座图中的 4 个点进行相位和振幅的编码，在档案数据传输过程中，实现离散调制和连续变量量子密钥分配方案。在此基础上，结合量子信息理论和 Shannon 信息理论，以及连续变量量子信号的特点进行安全性方面的理论分析，特别是分析离散调制下的连续变量量子密钥分配方案的安全性，建立这种情况下的档案数据安全性理论模型。

档案数据转换成量子信号后，参照光学编码技术，从技术上实现量子信号的 DPSK、4PSK 或 ASK 编码。在此基础上，采用 DFB 激光器作为相干光源产生相干态量子信号，通过 Mach- Zehnder 调制器采用图光学机制实现对量子信号的 DPSK 编码和 ASK 编码，随机输出依赖于相位或者振幅编码的量子比特。在接收端利用解码器输出信号，并利用平衡接收机检测信号，最终获取档案数据。

这个过程的光学实现比较简单，例如 DPSK 可采用相位调制器实现，项目组已经实现的“基于连续变量的量子密码综合平台”便是采用这种方式，项目在这个平台的基础上，通过改变编码调制方式，以及下面将提到的电路控制方式实现连续变量量子密钥分配系统的高速最终成码率，并提升传输距离。

离散变量和连续变量量子密码中同样存在安全性问题。在连续变量量子密码中，安全性分析更复杂，目前针对连续变量密码的安全性分析还不够透彻。不过，针对个体攻击的攻击策略已经有比较成熟的分析，文献中已经证明这种情况下是安全的。

3.2 数字档案传输电路模块

不管是离散变量还是连续变量量子密码中，控制电路模块都起着重要的作用。两者虽有一定的差异，但最终成码率和传输距离以及误码率都与这个模块有着紧密的联系。考虑到电路控制模块的重要性，项目组利用 FPGA 技术研制出高速的控制模块，包括高速的数 / 模、模和数据处理模块。利用所研制的模块，可以实现不依赖于计算机的量子密钥分配模块，从整体上提升连续变量量子密钥分配模块的性能和最终成码率。档案数据高速信号处理模块的原理结构如图 2 所示。

控制电路中还包括对 Homodyne 检测器中后期信号处理的电路，这部分属于高速探测技术方面的问题。该电路模块主要包括两个部分：一是基于 DSP 技术来实现对 Homodyne 检测器的高速采样与处理，该部分参考传统相干光通信中的 DSP- based Homodyne 检测技术；二是用于对检测模块的信号放大以及过噪声的抑制，项目组引入随机共振新技术，以大幅提

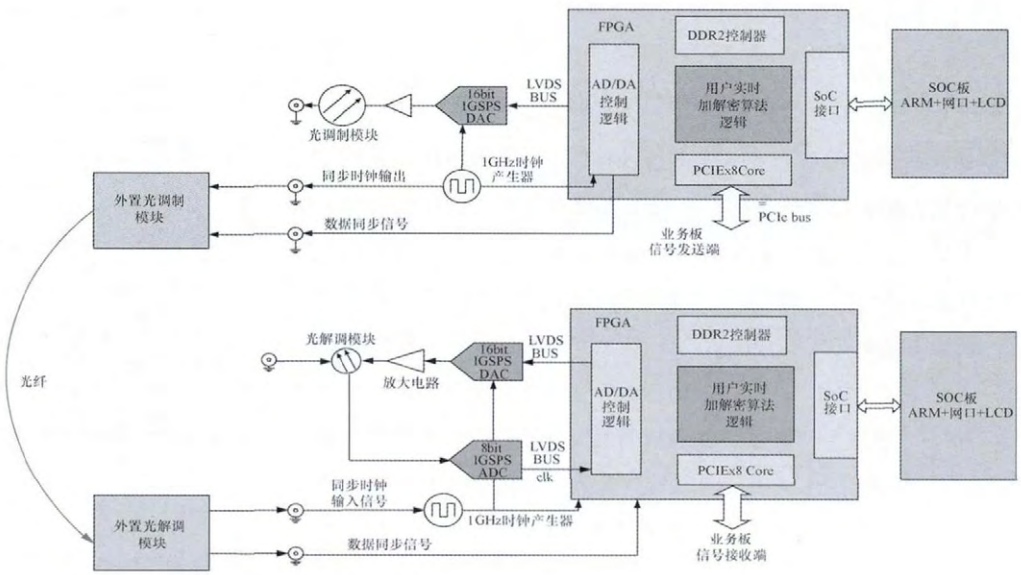

图 2　连续变量量子密钥分配系统的驱动电路

升检测信号的信噪比。

3.3 数字档案传输软件模块

档案数据传输系统应用模块中，秘密协商是一项非常重要的技术，它不但涉及量子密钥分配系统的效率、成码率和传输距离，而且也影响到系统的安全性。在实际应用中，量子密钥分配中的秘密协商算法是目前影响最终成码率的主要技术瓶颈。结合连续变量量子密钥分配的特点，利用LDPC技术研制出高效的连续变量量子密钥分配中的秘密协商算法，开发高效的软件模块。连续变量量子密钥分配技术的秘密协商软件模块，需要达到最佳转化效率；还需要考虑软件模块与硬件模块的融合性，使之成为一个整体。

量子密钥分配的软件模块的研制中，除了秘密协商模块外，还需要解决前面提到的相位补偿、偏振补偿方面的算法和软件实现。其中相位补偿和偏正补偿主要用于抵抗信道和检测器中过噪声的影响，提升系统的稳定性和鲁棒性。

3.4 数字档案传输样机系统

主要目标是研制出高速安全的连续变量量子密钥分配模块，为需要传输的档案数据进行加密，在接收端进行解密，再解析并还原出档案数据。为此，在前面所提方案和安全性分析的基础上，利用项目中所发展的高效秘密协商算法以及软件模块，研究高速安全稳定的连续变量量子密钥分配模块。

4 实验过程及效果分析

档案数字安全传输主要是期望在校内对公用户数据传输时运用，实验主要是以中南大学数字档案馆公共服务平台传输电子档案原文进行测试，公共服务平台将档案用户分为三类：个业务用户，面对校内外所有档案用户；校内对公用户，校内职工因工需要办理档案业务的人员；机构认证用户。校内对公用户是以校园信息门户进行校园卡身份验证，获得授权访问数字档案馆的用户。相对来说，用户身份已被确认，接下来仅需要在数据传输过程中保密即可。需要传递的档案数据，主要是档案的电子文件，目前以PDF、TIFF、JPG等格式为主。

4.1 档案数据传输过程

以中南大学档案馆为例，校内对用户在远程通过校园信息门户，以校园卡登陆公共服务平台，选择了业务信息或者查询到需要的电子档案之后提交申请，档案馆管理人员在数字档案馆管理平台收到请求后，核实身份并将电子档案授权给用户阅读。如果直接传输到用户端，涉密档案或有隐私信息的档案，就可能会泄露信息。安全传输过程如下：⑴ 连续变量QKD分配密钥；⑵ 通过光纤传输；⑶ 节点监控；⑷ 解析还原数据。

4.2 实验效果分析

通过数据分析，已经可实现如下的技术指标：档案数据传输距离27.2公里，最终成码率10kbps。但是，当一个实验室系统应用于实际电信光通信系统时，由于环境因素的影响，还有一些工程技术方面的问题需要解决，例如噪声扰动、相位漂移、效率等方面的问题，课题组将利用已有的基础设施（铁道校区和主校区之间的光纤）开展连续变量量子密钥分配模块的鲁棒性、稳定性和效率等方面的相关问题研究。

5 研究展望

随着云计算和大数据时代的到来，以及社会档案意识的提高，人们对档案信息的需求也不断增长，对便捷办理档案业务和快速获取档案信息的渴望越来越强烈[10]。如何建设档案服务体系和档案安全体系，如何解决档案服务与档案安全的巨大矛盾，这是档案界需要长期思考和探索的问题。课题组为档案数据传输过程的数据安全问题进行研究和探索，基于连续变量量子密码通信的档案数据安全传输技术，为全面构建档案安全体系打下基础，为最大程度提升档案远程服务能力提供保障，也从更深的层次上解决了档案方便利用与档案数据安全的矛盾，抛砖引玉，使档案行业引入更多的先进信息技术来解决档案问题。

参考文献：
[1] C. H. Bennett and G.Brassard. Quantum cryptography: Public key distribution and coin tossing. In Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, 1984, (IEEE, New York, 1984), pp. 175- 179.
[2] D. Mayers. Unconditional security in quantum cryptography. Journal of the ACM, 2001, 48:351- 406.
[3] H. K. Lo and H. F. Chau. Unconditional security of quantum key distribution over arbitrarily long distances. Science, 1999, 283:2050- 2056.
[4] P.W. Shor and J. Preskill. Simple proof os security of the BB84 quantum key distribution protocol. Physical Review Letters, 2000, 85:441- 444.
[5] H. Inamori, L. Rallan, and V. Vedral. Security of EPR- based quantum cryptography against incoherent symmetric attacks. preprint quant- ph/0103058.
[6] E. Biham, M.Boyer, P. O. Boykin, T. Mor, and V. Roychowdhury. A proof of the security of quantum key distribution. preprint quant- ph/9912053.
[7] X. Wang. Beating the photon- number- splitting attack in practical quantum cryptography. Physical Review Letters, 2005, 94:230503.
[8] 易智. 基于双模压缩态的量子保密通信协议[D]. 上海：上海交通大学，2008
[9] J. Lodewyck, T. Debuisschert, R. Tualle- Brouri, and Philippe Grangier. Controlling excess noise in fiber- optics continuous- variable quantum key distribution. Physical Review A, 2005, 72:050303(R).
[10] 向禹. 基于用户需求的高校档案在线服务平台的设计与实现[J].农业图书情报学刊，2015(09)