PONTIFÍCIA UNIVERSIDADE CATÓLICA
DO RIO DE JANEIRO

Guilherme Barreto Xavier

Esquemas de modulação para distribuição quântica de chaves com codificação de freqüência

Dissertação de Mestrado

Dissertação apresentada como requisito parcial para obtenção do título de Mestre pelo Programa de Pós-Graduação em Engenharia Elétrica da PUC-Rio.

Orientador: Jean Pierre von der Weid

Rio de Janeiro, fevereiro de 2005

Guilherme Barreto Xavier

Esquemas de modulação para distribuição quântica de chaves com codificação de freqüência

Dissertação apresentada como requisito parcial para obtenção do título de Mestre pelo Programa de Pós-Graduação em Engenharia Elétrica da PUC-Rio. Aprovada pela Comissão Examinadora abaixo assinada.

Jean Pierre von der Weid
Orientador
PUC-Rio

Rogério Passy
PUC-Rio

Paulo Henrique Souto Ribeiro
UFRJ

Patrícia Lustoza de Souza
PUC-Rio

José Eugenio Leal
Coordenador(a) Setorial do Centro Técnico Científico - PUC-Rio

Rio de Janeiro, 24 de fevereiro de 2005

Guilherme Barreto Xavier

Formado em Engenharia Elétrica com ênfase em telecomunicações e eletrônica pela PUC-Rio em 2003. Suas atuais áreas de interesse incluem teoria da informação quântica, comunicação quântica e metrologia óptica.

Ficha Catalográfica

Xavier, Guilherme Barreto

Esquemas de modulação para distribuição quântica de chaves com codificação de frequência / Guilherme Barreto Xavier ; orientador: Jean Pierre von der Weid. – Rio de Janeiro : PUC-Rio, Departamento de Engenharia Elétrica, 2005.

98 f. : il. ; 30 cm

Dissertação (mestrado) – Pontifícia Universidade Católica do Rio de Janeiro, Departamento de Engenharia Elétrica .

Inclui bibliografia.

1. Engenharia Elétrica – Teses. 2. Criptografia quântica. 3. Distribuição quântica de chaves. 4. Teoria de informação quântica. 5. Comunicação quântica. 6. QKD. I. Weid, Jean Pierre Von der. II. Pontifícia Universidade Católica do Rio de Janeiro. Departamento de Engenharia Elétrica . III. Título.

CDD: 621.3

Agradecimentos

Ao Prof. Jean Pierre, pela orientação, pelos ensinamentos pessoais e profissionais e pela oportunidade de poder trabalhar com QKD.

Aos meus pais Álvaro e Luiza e meu irmão Bernardo, pelo apoio incondicional sem o qual eu não teria feito esse trabalho.

A minha namorada, amiga e companheira Bruna, por ter sido meu alicerce durante a dissertação e por sempre ter me dado força para eu trabalhar no que eu gosto.

Ao pessoal do laboratório (em ordem alfabética), Amália, Breno, Claiton, Djeisson, Filipe Forte, Janaína, Mauro, Marçal e Temporão pelo apoio, pelas discussões e pelas piadas. Em especial ao Giancarlo por estar sempre pronto e com paciência a ajudar.

Aos Profs. Patrícia e Maurício, por terem me apoiado na área acadêmica desde a época da iniciação. Ao pessoal do LabSem pela força sempre que precisava em especial ao Iracildo e a Maria Cristina.

A todo o pessoal do CETUC em especial ao Brás. A galera da instrumentação por sempre ter uma ferramenta pra emprestar e principalmente ao Rodrigo por ter desenhado os compartimentos dos contadores de fótons, que finalmente poderão ser utilizados.

A todos os amigos que me deram apoio e acreditaram em mim. A minha cunhada Paula por ter me recebido diversos fins de semana.

A CAPES pelo apoio financeiro.

Resumo

Xavier Barreto, Guilherme. **Esquemas de modulação para distribuição quântica de chaves com codificação de freqüência.** Rio de Janeiro, 2005. 98p. Dissertação de Mestrado - Departamento de Engenharia Elétrica, Pontifícia Universidade Católica do Rio de Janeiro.

A criptografia quântica foi proposta como uma solução para o problema da distribuição de chaves criptográficas com segurança total garantida pelos princípios da mecânica quântica. Através dessa técnica é possível saber se um espião tentou interceptar a transmissão, o que é impossível utilizando técnicas de transmissão clássicas. Nesse trabalho foi feito um breve resumo da teoria de criptografia quântica, de suas técnicas de transmissão e dos problemas tecnológicos enfrentados. Foi analisada em detalhes a técnica de transmissão de qubits utilizando codificação de freqüência e feita uma comparação dos diferentes esquemas de modulação frente aos protocolos BB84 e B92. Foi demonstrado que os dois esquemas de modulação existentes (AM-AM e PM-PM) são na realidade equivalentes e foi proposto um novo esquema, o AM-PM o único que suporta o protocolo BB84 clássico. Medidas foram realizadas classicamente nos formatos AM-AM e AM-PM.

Palavras-chave

Criptografia quântica; distribuição quântica de chaves; QKD; teoria de informação quântica; comunicação quântica.

Abstract

Quantum cryptography has been proposed as a solution to the cryptographic key distribution problem with absolute security guaranteed by the principles of quantum mechanics. Through this scheme it is possible to find out whether a spy tried to eavesdrop on the transmission, which was impossible to discover using classical transmission techniques. In this work a brief review of quantum cryptography theory, transmission techniques and technological problems involved were performed. It was analyzed in detail the transmission technique employing frequency coding, and a comparison was made between the different modulation schemes and the BB84 and B92 protocols. It was demonstrated that the two existing modulation formats (AM-AM and PM-PM) are in fact equivalent and a new format (AM-PM) was proposed, the only one able to accommodate classical BB84. Classical measurements were performed on the AM-AM and AM-PM formats.

Keywords

Quantum cryptography; Quantum key distribution; QKD; Quantum information theory; Quantum communications.

Sumário

Lista de figuras

Lista de tabelas

Lista de abreviaturas

LED – Diodo Emissor de Luz (*Light Emitting Diode*).

QKD – Distribuição de Chaves Quânticas (*Quantum Key Distribution*).

EPR – Einstein Podolsky Rosen

BSM – Medição no Estado de Bell (*Bell-State Measurement*)

RSA – Rivest Shamir Adleman

QED – EletroDinâmica Quântica (*Quantum ElectroDynamics*).

NMR – Ressonância Nuclear Magnética (*Nuclear Magnetic Ressonance*)

PBS – Divisor de Feixes de Polarização (*Polarization Beam Splitter)*

SPAD – Detectores Avalanche para Fótons Unitários (*Single Photon Avalanche Detector*).

PMD - Dispersão dos Modos de Polarização (*Polarization Mode Dispersion*).

PMF – Fibras Mantenedoras de Polarização (*Polarization Maintaining Fibers*).

DS – Dispersão Deslocada (*Dispersion Shifted*).

POVM – Medição do Valor do Operador Positivo (*Positive Operator Value Measurement*).

WCP – Pulsos Fracos Coerentes (*Weak Coherent Pulses*).

PNS – Divisão do Número de Fótons (*Photon Number Splitting*).

RF – Radio Freqüência (*Radio Frequency*).

CW – Freqüência Contínua (*Continuous Wave*).

WDM – Multiplexação por Comprimento de Onda (*Wavelength Division Multiplexing*).

OSA – Analisador de Espectro Óptico (*Optical Spectrum Analyzer*).

ESA – Analisador de Espectro Elétrico (*Electrical Spectrum Analyzer*).

GPIB – *General Purpose Interface Bus*

EA – Electro-Absorção (*Electro-Absorption*).