

PONTIFÍCIA UNIVERSIDADE CATÓLICA
DO RIO DE JANEIRO



Guilherme Barreto Xavier

**Esquemas de modulação para distribuição quântica de
chaves com codificação de frequência**

PUC-Rio - Certificação Digital Nº 0321228/CA

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 frequência**

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

Todos os direitos reservados. É proibida a reprodução total ou parcial do trabalho sem autorização da universidade, do autor e do orientador.

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 frequência**. 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 frequência 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

1	Introdução	14
1.1	Criptografia Quântica	16
1.2	Teleportação quântica	17
1.3	Computação quântica	19
2	Criptografia: do clássico ao quântico	22
2.1	Introdução	22
2.2	Porquê a criptografia clássica é vulnerável.	22
2.3	A teoria quântica entra em cena	26
2.3.1	O protocolo BB84	27
2.3.2	O protocolo EPR	33
2.3.3	Codificação em fase	35
2.3.4	O protocolo B92	40
2.3.5	Sistemas “Plug and Play”	41
2.3.6	Codificação por frequência	44
3	Sistemas reais	46
3.1	Transmissão e recepção	46
3.1.1	As fontes ópticas	46
3.2	Como detectar um fóton?	49
3.2.1	Princípio de operação do APD	50
3.2.2	O APD como SPAD	50
3.2.3	Desempenho dos SPADs	54
3.3	QBER	57
3.4	Ataques	60
3.4.1	Ataques incoerentes	61
3.4.2	Ataques coerentes	63
4	Codificação por frequência	65
4.1	Princípio de operação	65

4.2 Sistema PM-PM	67
4.3 Sistema AM-AM	74
4.4 Sistema AM-PM	80
4.5 Considerações finais sobre a codificação por frequência	83
5 Resultados experimentais	85
5.1 A montagem	85
5.2 Sistema AM-AM	87
5.3 Sistema AM-PM	89
5.4 Comentários	90
6 Conclusões e considerações finais	94
7 Referências bibliográficas	96

Lista de figuras

Figura 1: Esquema simplificado de um sistema de teleportação de <i>qubits</i> utilizando fótons.	19
Figura 2: Idéia do “ <i>one-time pad</i> ”.	24
Figura 3: Princípio de funcionamento do esquema de criptografia clássica pública.	25
Figura 4: Esquema de uma possível transmissão de <i>qubits</i> codificados por Alice utilizando uma base ortogonal de polarização.	29
Figura 5: Implementação do BB84.	30
Figura 6: Sistema de criptografia quântica utilizando pares EPR para a transmissão dos <i>qubits</i> .	35
Figura 7: Idéia inicial de um esquema para QKD utilizando codificação de fase.	37
Figura 8: Esquema modificado do sistema para transmissão de <i>qubits</i> utilizando codificação de fase composta de dois “meio-interferômetros”.	38
Figura 9: Sistema “ <i>Plug and Play</i> ” para a transmissão de <i>qubits</i> utilizando a codificação de fase.	42
Figura 10: Situação esquemática da emissão de WCPs de um laser pulsado para $\mu = 1$.	47
Figura 11: Esquema de transmissão de <i>qubits</i> utilizando um cristal não-linear para a geração de fótons.	49
Figura 12: Esquema ilustrativo da estrutura de um APD indicando as regiões de ganho e absorção.	51
Figura 13: Circuitos para operação dos APDs como SPADs.	52
Figura 14: Gráfico dos coeficientes de absorção para diversas ligas semicondutoras em função do comprimento de onda.	55
Figura 15: Ataque PNS realizado por Eva em um sistema de QKD.	62
Figura 16: Esquema de ataque coletivo praticado por Eva.	64
Figura 17: Esquema de transmissão de <i>qubits</i> utilizando codificação de frequência.	66
Figura 18: Espectro de frequências gerado através de simulação no	

<i>MATLAB</i> para quatro valores de $\Delta\varphi$. O termo de propagação foi assumido como zero.	72
Figura 19: Diagrama de um modulador MZ com os sinais ópticos de entrada e saída.	75
Figura 20: Espectros do sinal na saída do modulador de Bob.	79
Figura 21: Espectro do sistema AM-PM para os mesmos quatro valores de $\Delta\varphi$.	82
Figura 22: Esquema experimental utilizado nas medidas.	86
Figura 23: Espectro obtido a partir do ESA para o sistema AM-AM.	87
Figura 24: Evolução da intensidade das bandas laterais em função do desvio de frequência imposto por Alice e Bob para o sistema AM-AM	88
Figura 25: Espectros para o sistema AM-PM.	89
Figura 26: Evolução das intensidades em função do desvio de frequência do sistema AM-PM.	90
Figura 27: Evolução da intensidade das bandas laterais para um sistema AM-AM utilizando um modulador de EA em Alice.	91
Figura 28: Intensidades para as bandas laterais para o esquema AM-AM operando em modo pulsado.	93
Figura 29: Análoga à figura 28, porém para o esquema AM-PM.	93

Lista de tabelas

Tabela 1: <i>Sifted Key</i> gerada a partir de um conjunto de bits a ser enviado após a verificação das bases coincidentes.	33
Tabela 2: Esquema de utilização do protocolo BB84 com codificação de fase.	39
Tabela 3: Gama de possibilidades para o sistema PM-PM fazendo o termo de propagação igual a zero.	73
Tabela 4: Resultados possíveis para o sistema AM-PM.	81

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 Resonance*)

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 Frequência (*Radio Frequency*).

CW – Frequência 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*).

GPIO – *General Purpose Interface Bus*

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