UNIVERSIDADE FEDERAL DO CEARÁ
CENTRO DE TECNOLOGIA
DEPARTAMENTO DE FÍSICA
CURSO DE PÓS-GRADUÇÃO EM FÍSICA

ESTUDO DO DESEMPENHO DE FILTROS ACÚSTICO-ÓPTICOS SINTONIZÁVEIS COMO COMPONENTES BIESTÁVEIS E SUA UTILIZAÇÃO NA CRIPTOGRAFIA EM REDES ÓPTICAS.

FORTALEZA
2009

KARLO DAVID ALVES SABÓIA

ESTUDO DO DESEMPENHO DE FILTROS ACÚSTICO-ÓPTICOS SINTONIZÁVEIS COMO COMPONENTES BIESTÁVEIS E SUA UTILIZAÇÃO NA CRIPTOGRAFIA EM REDES ÓPTICAS.

Tese de doutorado apresentada ao Departamento de Física da Universidade Federal do Ceará, como parte dos requisitos para a obtenção do Título de Doutor em Física.

Orientação: Dr. Antônio Sérgio Bezerra Sombra.

FORTALEZA
2009

Dedico este trabalho primeiramente à memória de meus avós José Mourão da Silva, Maria Creusa Sabóia e Silva e Maria Alves de Brito, não só pelo imenso carinho a mim dedicado mas, principalmente, por terem sido os principais responsáveis pela herança moral sob a qual guio minha existência.

Àqueles que nunca acreditaram em minhas fraquezas e sempre me tomaram como um vencedor, mesmo diante de meus momentos de clara derrota: minha mãe, Maria Raimunda Alves Sabóia, meu pai, Francisco das Chagas Sabóia e Silva, minhas irmãs, Kamilla Alves Sabóia e Klarissa R. Alves Sabóia.

A todos aqueles que me apoiaram ao longo desses quase quinze anos de luta, longe de "casa". Seria complicado citar todos, mas eu gostaria de explicitar alguns: Maria do Desterro Alves de Brito, Fernando Moreira Brito, Paulo Moreira Brito, Osmar Moreira Brito, Maria Irismar Sabóia, Antônio Rodrigues Vale, Tomás Aguiar Pinto, Zilene Sabóia e Silva, David Sabóia da Silva, José Liberato Sabóia e Silva, Jaime Girão Junior e Heliane Thomeny Girão.

Àqueles diante dos quais eu não suportaria falhar, meus grandes amigos João Paulo Ferreira Lima, Cristiano Oliveira Rodrigues, Ocion Doroteu de Macedo, Adauto Doroteu de Macedo, Fábia Sampaio de Oliveira, Sara Menezes de Oliveira.

À minha fiel companheira de quase dez anos de luta e sofrimento e que, pelos poucos momentos bons que pude lhe proporcionar, nunca deixou de acreditar em mim, em nós; minha amada esposa Helainne Thomeny Girão.

Àquela que, acima de tudo nesse mundo, é o que tenho de mais valioso, de mais vivo, de mais belo; àquela que é tão essencial a minha vida quanto o ar que eu respiro; àquela que é minha carne, meu sangue, meu espírito; minha filha Sara. Que este trabalho lhe sirva não como um exemplo de até onde deva ir, mas como uma barreira óbvia e irrisória em sua escalada de montes infinitamente mais altos.

AGRADECIMENTOS

Meus sinceros agradecimentos a CAPES (Coordenação de Aperfeiçoamento Pessoal de Nível Superior) pelo financiamento desta pesquisa por meio da bolsa de doutorado a mim cedida. Agradeço também aos meus colegas de trabalho que fazem parte do grupo LOCEM, dentre os quais gostaria de destacar Dr. Cícero Saraiva Sobrinho, M^{e}. José Wally M. Menezes, Dr. Wilton B. Fraga e M^{e} Alisson C. Ferreira

Gostaria de agradecer ao colega Bruno Bastos Sales pelas correções no *Abstract*, à Prof. Érica Soares e à minha esposa Helainne T. Girão pela revisão deste trabalho e por seus significativos conselhos que contribuíram para a melhoria do mesmo.

Eu também não poderia deixar de agradecer à Sra. Maria Joselita Ramos Vitorino, pelos infinitos conselhos que tanto me ajudaram no desenvolvimento de um modo mais sóbrio de pensar; e, nesse contexto, gostaria de agradecer aos professores responsáveis pela minha formação, dos quais eu gostaria de destacar Dr. Raimundo Valmir Leite Filho, M^{e} José Carlos de Souza Carneiro, Dr. Ricardo Renan Landim de Carvalho, Dr. Newton Theóphilo de Oliveira e Dr. Júlio Auto Neto.

Gostaria de agradecer também, pelo imenso apoio intelectual, aos meus colegas: Alan Silva de Menezes, Victor Hugo Bezerra, Francisco Ednilson Alves dos Santos, Aristeu, Leandro Ibiapina Beviláqua, Kátia Andrade, Bruno Tavares de Oliveira Abagaro, Bruno Bastos Sales, Francisco Wagner Vasconcelos da Costa, Francisco Franciné Maia Júnior, Cláudio Lucas Nunes de Oliveira, Felipe de Freitas Munarin, Marcelo Zimmer e Vladimir V. de Assis.

E em especial, eu gostaria de agradecer ao Prof. Dr. Antônio Sérgio Bezerra Sombra por sua inestimável orientação, marcante humildade, constante sobriedade e, principalmente, por sua imensa compreensão ante as imprevisibilidades da vida.

“I haven't failed, I've found 10,000 ways that don't work.”

Thomas Edison

RESUMO

O Estudo do Desempenho de Filtros Acústico-Ópticos Sintonizáveis (AOTF) como Componentes Biestáveis e sua Utilização na Criptografia em Redes Ópticas apresenta, primeiramente, um estudo analítico e numérico de tais filtros destacando suas principais propriedades de transmissão e analisando seu comportamento devido aos efeitos não-lineares e o surgimento da biestabilidade óptica quando um sistema de *feedback* é introduzido. Em seguida, propõe o uso do AOTF, somado à modulação de pulsos ultracurtos por posição (PPM) e por amplitude (PAM), simultaneamente, para gerar um sistema criptográfico a ser utilizado em redes ópticas. As simulações numéricas foram realizadas utilizando-se o método de Runge-Kutta de Quarta Ordem. Os resultados obtidos para o estudo da biestabilidade mostraram a dependência da curva de histerese com relação ao produto da constante de acoplamento (κ) pelo comprimento do dispositivo (ξ_L) e ao fator de conversão potência-constante de propagação (G). Mostrou-se que o intervalo da biestabilidade varia significativamente tanto com G como com $\kappa\xi_L$, mas suas contribuições são diferentes. A variação do produto $\kappa\xi_L$ aumenta o tamanho do intervalo da biestabilidade, enquanto que o aumento de G faz com que a biestabilidade ocorra para potências iniciais cada vez menores. Os resultados obtidos no estudo do AOTF como criptógrafo mostraram que é possível definir um par de parâmetros, chamado par PPM/PAM (ε_{PPM}, ε_{PAM}), diretamente relacionado com as modulações usadas no processo, que servirá como elemento fundamental para a comunicações entre dois usuários em uma rede óptica usando um AOTF para codificar a mensagem e outro para decodificar.

Palavras-chave: Filtros acústico-ópticos sintonizáveis. Biestabilidade. Criptografia.

ABSTRACT

The performance of acoustic-optic tunable filters (AOTF) as a bistable component, applied to cryptography in optical networks, has been studied with analytical and numerical methods. Initial investigations of such filters highlighted their main transmissions, and analyzed their behavior by nonlinear effects with formation of optical bistability when a feedback was introduced in the system. Subsequently, it was proposed the use of an AOTF device, together with simultaneous modulation of ultrashort pulses by position (PPM) and amplitude (PAM), for generation of a cryptographic system for application in optical networks. Numerical simulations were performed using the Runge-Kutta fourth order method. The results for the study of bistability showed the dependence of the hysteresis curve with respect to the product of coupling constant (κ) by the length of the device (ξ_L) and the conversion power-coupling constant factor (G). It was shown that the range of bistability varies significantly with both G and $\kappa\xi_L$. The variation of the product $\kappa\xi_L$ directly increases the size of the bistability range while the increase in G causes the bistability occurrence for initial powers to decrease. The results obtained in the study of the AOTF as a cryptographer showed that it is possible to define a pair of parameters, called PPM/PAM pair (ε_{PPM}, ε_{PAM}), directly related to the modulations used in the process, which will serve as key to communications between two users in an optical network. The device would be used to encode and decode data.

Key-words: Acoustic-optic tunable filter. Bistability, Cryptography.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SÍMBOLOS

α – Coeficiente de atenuação em um AOTF não ideal.

$\Delta\beta$ – Diferença ou descasamento de fase longitudinal.

β – Componente de fase ou constante de propagação de uma onda eletromagnética propagando-se na direção *z*.

$\beta^{(m)} = \left(\frac{d^m \beta}{d \omega^m} \right)_{\omega = \omega_o}$ – Componente de ordem m da expansão em serie de Taylor de β.

$\beta^{(2)}$ – Parâmetro de ordem mais baixa da dispersão da velocidade de grupo (GVD).

ξ_L – Comprimento de um AOTF ou comprimento total de interação acústico óptica.

$C_j = \mathbf{E}_j^* \exp(i\beta_j z)$, para $j = 1$ ou 2.

c – Velocidade da luz no vácuo.

E – Vetor campo elétrico de uma onda eletromagnética.

ε – Tensor de permissividade dielétrica do meio.

$\Delta\varepsilon$ – Variação no tensor de permissividade dielétrica.

ε_0 – Permissividade dielétrica do espaço livre.

ε_{PAM} – Adição na amplitude para a modulação PAM.

ε_{PPM} – Deslocamento temporal para a modulação PPM.

Δf_{AOTF} – Largura de banda total do filtro no ponto de metade da máxima intensidade.

G – Fator de conversão potência-constante de propagação.

H – Vetor campo magnético de uma onda eletromagnética.

i – Utilizado em números complexos para representar a sua parte imaginária.

I – Intensidade do campo aplicado.

I_i – Representa a intensidade da potência na entrada do AOTF no estudo da biestabilidade.

I_o – Representa a intensidade da potência na saída do AOTF no estudo da biestabilidade.

$\kappa = |\kappa_{12}| = |C_{12}|$ – Constante de acoplamento linear entre os dois modos.

$\mathbf{K}$ – Vetor de onda acústica.

$\mathbf{k}_1$ e $\mathbf{k}_2$ – Vetores de onda da luz incidente e difratada, respectivamente.

L – Comprimento de referência para o AOTF.

L_D – Comprimento de dispersão.

L_{NL} – Comprimento de não linearidade.

μ_0 – Permeabilidade magnética do espaço livre.

μ – Tensor de permeabilidade magnética do meio.

$\Delta n = n_1 - n_2$ – Birefringência do meio.

N – Define a ordem de um sóliton.

n_1 e n_2 – Índices de refração associados com a ondas incidente e difratada, respectivamente.

n – Índice de refração do meio.

n_{NL} – Índice de refração não linear.

n_L – Índice de refração linear.

P – Potência óptica em função da distância propagado z [$P(z = 0) = P_0 = P_{entrada}$].

$\mathbf{P}_{\mathrm{P}}$ – Vetor de polarização devido a perturbação.

$\mathbf{P}_{\mathrm{L}}$ – Vetor de polarização linear.

$\mathbf{P}_{\mathrm{NL}}$ – Vetor de polarização não linear.

$\mathbf{P} = \mathbf{P}_{\mathrm{L}} + \mathbf{P}_{\mathrm{NL}}$ – Vetor de polarização para um meio sem a perturbação periódica.

$\mathbf{P}_{\mathrm{T}} = \mathbf{P}_{\mathrm{L}} + \mathbf{P}_{\mathrm{NL}} + \mathbf{P}_{\mathrm{P}}$ – Vetor de polarização total do meio, incluindo a perturbação periódica.

p_{qr} – Coeficiente acústico óptico (dependem das características intrínsecas do meio).

ρ – Valor final do perfil de não linearidade crescente.

ρ_o – Valor final ótimo do perfil de não linearidade crescente.

Q – Representa o perfil de não linearidade crescente da auto modulação de fase.

$\mathbf{r}$ – Vetor que determina a posição espacial do campo elétrico.

S_r – Tensor acústico no material.

Δt_j – Duração temporal total de um pulso no ponto de metade da máxima intensidade (FWHM), onde $j = 1$ ou 2.

Δt_0 – Duração temporal de um pulso no ponto de intensidade (P_0/e).

T – Coeficiente de conversão de energia entre os dois modos ou transmissão.

t – Tempo medido em um referencial propagando-se na mesma velocidade do pulso.

v – Velocidade do som no meio.

v_g – Velocidade de grupo.

ω – Freqüência qualquer do espectro eletromagnética.

ω_1 e ω_2 – Freqüências da onda incidente e difratada, respectivamente.

ω_o – Freqüência óptica central de um pulso ($\omega_o = 2\pi f_o$).

ω_c – Freqüência óptica central de atuação ou selecionada pelo filtro ($\omega_c = 2\pi f_c$).

$\Omega = 2\pi f_a$ – Freqüência da onda acústica.

$\chi^{(1)}$, $\chi^{(2)}$ e $\chi^{(3)}$ – Susceptibilidades de 1ª, 2ª e 3ª ordem, respectivamente.

z – Distância propagada pela onda acústica e as amplitude A_1 e A_2.

∇ – Vetor utilizado para o cálculo do rotacional ou divergente de outro vetor.

Λ – Período de uma perturbação dielétrica expandida em uma Série de Fourier.

$\otimes$ – Representa o produto tensorial.

θ_j – Ângulo entre o vetor de onda $\mathbf{k}_j$ ($j = 1$ ou 2) e as frentes de onda acústica.

ϕ – Fase total do campo óptico.

ϕ_{NL} – Mudança de fase não linear do campo óptico.

$\delta\omega_0$ – "*chirp*" inicial de fase.

γ – Coeficiente de não linearidade básica.

LISTA DE ABREVIATURAS E SIGLAS

AES – do inglês *Advanced Encryption Standard*;

AO – acústico-óptico;

AOTF – do inglês *Acoustic Optic Tunable Filter;*

AT&T – do inglês *American Telegraph and Telephone Company*;

CW – do inglês *Continuous Wave*;

chirp – dentro do contexto, significa uma mudança na freqüência óptica instantânea através do perfil do pulso, devido a uma dependência temporal da fase;

crosstalk – dentro do contexto, significa a possível interferência de energia entre os modos acoplados;

DES – do inglês *Data Encryption Standard*;

FWHM – do inglês *Full Width Half Maximum*;

GVD – do inglês *group velocity dispersion*;

IBM – do inglês *International Business Machines*;

laser – do inglês *light amplification by stimulated emission of radiation*.

NSA – do inglês *National Security Agency*;

PAM – do inglês *Pulse-amplitude modulation.*

PPM – do inglês *Pulse-position modulation.*

RF – radio freqüência.

SAW – do inglês *Surface Acoustic Wave*.

SPM – do inglês *Self Phase Modulation*.

TE – do inglês *Transverse Electric*.

TM – do inglês *Transverse Magnetic*.

WDM – do inglês *Wavelength Division Multiplexing*.

XPM – do inglês *Cross-Phase Modulation*.

SUMÁRIO

INTRODUÇÃO

Seria pouco arriscado afirmarmos que uma das fundamentais características que define o mundo moderno é a incrível facilidade de se trocar informações a altas velocidades com qualquer outra parte do globo terrestre. Computadores estão presentes em basicamente quase todas as esferas sociais; telefones celulares tornaram-se um bem obrigatório em praticamente qualquer tipo ou nível profissional; transações bancárias são realizadas por qualquer cidadão comum em qualquer lugar que ele estiver. De uma forma geral, todos os tipos de transações financeiras modernas são processadas automaticamente em uma escala gigantesca, assim como dados médicos, transações de compras, etc., através da *internet*. Se acrescentarmos a esse quadro uma parcela significativa da população humana que faz uso da telefonia e da *internet* na sua vida cotidiana por já fazer enfim parte dela, temos um quadro ainda nada próximo da quantidade de informações a circular diariamente por nosso planeta.

Assim, o momento atual exige uma busca intensa por métodos mais rápidos para o processamento de tais informações, e é nesse contexto que surge o interesse de se conseguir dispositivos que funcionem totalmente no domínio óptico, funcionando como elementos capazes de tratar e/ou processar informação a velocidades ultra-rápidas. Destarte, pesquisadores têm se dedicado ao desenvolvimento de tecnologias de chaveamento ultra-rápido de dispositivos óticos, representando um impacto crescente na Engenharia Elétrica.

Somado ao problema do aumento da quantidade de informação comutada, faz parte ainda desse contexto a segurança no transporte de tais informações. Vale ressaltar que essa discussão prepondera sobre qualquer outro fator devido aos tipos de transações a serem utilizadas via *internet*. Entra-se, portanto, no domínio da Criptografia. Criptografia é a área da Criptologia que lida com técnicas baseadas em uma chave secreta para decifrar uma mensagem. Métodos criptográficos são requeridos quando se deseja proteger tais informações de serem recebidas e interpretadas por um usuário a quem elas não foram originalmente destinadas. O processamento de informações ópticas tem demonstrado um imenso potencial como promissora ferramenta em aplicações de segurança. Não apenas em sistemas totalmente ópticos, mas, mesmo em sistemas híbridos, processos criptográficos são sugeridos.

Torna-se óbvio ressaltar que é de suma importância a velocidade com que a informação não só é codificada, mas também decodificada. É justamente neste contexto que surge a necessidade de dispositivos totalmente ópticos. Assim, imergimos na presente problemática fazendo uso do Filtro Acústico-Óptico Sintonizável (AOTF) com guias de onda em substratos ópticos. O AOTF é um dispositivo que funciona a partir do princípio de interação acústico-óptica. Ele tem atraído grande atenção dentre outros aspectos por ser provavelmente o único filtro capaz de selecionar múltiplos comprimentos de onda simultaneamente, pois um único cristal pode acomodar múltiplas ondas acústicas de freqüências diferentes. Esta propriedade pode ser usada para construir roteadores de múltiplos comprimentos de onda, muito importante em redes WDM. Dessa forma, o AOTF é um dispositivo de grande versatilidade em redes ópticas e, em particular, no estudo de chaveamento de energia a níveis ultra-rápidos.

Fazendo uso das propriedades do AOTF somadas à modulação de pulsos ultracurtos por posição e amplitude simultaneamente, foi possível gerar um dispositivo que criptografasse uma mensagem e a lançasse com segurança por uma rede. A segurança de mensagens tem sido nos últimos anos um tópico de profunda importância para os meios de comunicação. Vários sistemas e dispositivos têm sido desenvolvidos ao longo da história da criptografia no sentido de garantir segurança absoluta as informações enviadas. Assim, o presente trabalho tem por objetivos fazer um breve estudo numérico e analítico das propriedades do AOTF e demonstrar numericamente o funcionamento do mesmo associado à modulação por amplitude (PAM) e por posição (PPM) no intuito de criar um sistema de proteção de mensagens.

O estudo numérico e analítico tem seu papel aqui no sentido de nos prover material teórico (e prático) para a completa compreensão do dispositivo a ser simulado, embasando assim a analise futura do uso do mesmo no processo criptográfico. A partir das equações de Maxwell aplicadas a meios anisotrópicos, encontramos um conjunto de equações acopladas definindo o modo de propagação no interior do AOTF. Será possível ver que apenas dois desses modos serão relevantes e o sistema de equações passa a ser resolvido a partir de métodos numéricos (usamos o de Runge–Kutta de quarta ordem), levando ainda em conta as condições iniciais obtidas na análise física do problema. Todas as simulação foram realizadas com pulsos ultracurtos (2ps).

O estudo numérico e analítico de filtros acústico-ópticos sintonizáveis utilizados na criptografia de pulsos ultracurtos, aqui proposto, requer uma exposição de conceitos de

diferentes áreas: o estudo de códigos, possibilitando o entendimento dos processos criptográficos básicos utilizados na transmissão de informações, a física, possibilitando o desenvolvimento teórico para o entendimento do efeito acústico-óptico e a engenharia, possibilitando o entendimento da construção do dispositivo em questão. Foi necessária então uma breve exposição, um breve estudo, das mesmas antes de apresentarmos a estrutura básica do modelo proposto à criptografia. Nesse sentido, o trabalho foi dividido da seguinte forma.

O Capítulo 1, Proteção de Informação, de caráter introdutório, tem como objetivo contextualizar o problema a partir de sua relevância história levando o leitor até um estágio geral da teoria criptográfica utilizada nos meios de comunicação e discute a importância do problema da proteção de mensagens. Conceitos básicos de criptografia são apresentados permitindo ao leitor entender a evolução dos sistemas criptográficos clássicos (na medida do possível, dentro do contexto histórico ao qual eles pertencem) e, por fim, ele é apresentado aos conceitos modernos de sistemas de chaves-públicas e aos procedimentos de controle de chave. Esses conceitos serão utilizados posteriormente quando discutirmos o processo criptográfico aqui proposto.

O Capítulo 2, Efeito Acústico-Óptico, traz o embasamento teórico para o entendimento do efeito acústico-óptico. As características e limitações de um dispositivo óptico podem ser entendidas, e apreciadas, somente através de um estudo da propagação eletromagnética através do meio óptico do qual é composto. As propriedades ópticas do meio são descritas pelos seus parâmetros materiais como, por exemplo, o tensor dielétrico, os coeficientes eletro-ópticos, as constantes fotoelásticas, e as susceptibilidades de ordem qualquer. Destarte, estuda-se a propagação eletromagnética em meios periódicos, uma vez que o principal componente no interior do AOTF é um cristal, e chega-se a um conjunto de equações acopladas. O capítulo finaliza discutindo o efeito fotoelástico e resolvendo o conjunto de equações acopladas para encontrarmos as informações sobre a intensidade e a polarização dos modos propagando no interior do dispositivo.

O Capítulo 3, Caracterização e Propriedade de um AOTF, faz uma abordagem sobre o próprio AOTF. Este capítulo baseia-se no estudo analítico e numérico deste dispositivo discutindo suas propriedades e comportamentos. Reunimos, portanto, o resultado de vários trabalhos sobre tal dispositivo, dentre eles trabalhos desenvolvidos pelo próprio autor, por

pesquisadores pertencentes ao grupo do autor e trabalhos diversos, com o intuito de tornar o conhecimento sobre tal dispositivo o mais completo possível. Destacamos nesse capítulo simulações recentes sobre o problema da biestabilidade no acústico-óptico.

O Capítulo 4, Processo Criptográfico, apresenta o processo criptográfico proposto neste trabalho. Lá, apresentamos o material mais significativo, a técnica utilizada para codificar pulsos ultracurtos sólitons (2ps), que se consiste basicamente em duas partes: a primeira é a redução do número de pulsos formando a mensagem original, através da modulação simultânea por posição e por amplitude. A cada quatro pulsos a formar a mensagem original, o processo de modulação reduzirá a quantidade para dois. A segunda é a passagem desses pulsos, assim modulados, através de um AOTF. Apenas um dos modos eletromagnéticos será lançado através da fibra como um pulso de informação. Ou seja, a informação de quatro pulsos será condensada em apenas um. O processo de recuperação se dará pela passagem por um segundo AOTF usando a chave correta para a recuperação dos quatro pulsos de informação iniciais. Ainda nesse capítulo, discutiremos a segurança de tal dispositivo com respeito ao ataque de usuários mal intencionados que desejarem quebrar o código.

O capítulo 5, de caráter conclusivo, apresenta as considerações finais a respeito do estudo analítico realizado nos capítulos 3 e 4. As conclusões a respeito da eficiência do dispositivo são reavaliadas e o capítulo finaliza com uma visão geral de sua aplicabilidade.

1 PROTEÇÃO DE INFORMAÇÃO

No ano de 1798, Napoleão Bonaparte almejava aumentar as posses do Império Francês com a expedição do Egito. Estrategicamente, ele também desejava evitar a comunicação do Império Britânico com a Ásia. Desse modo, uma grande força armada chegou ao Egito na primavera daquele mesmo ano e tomou Malta [1]. Cerca de um ano depois, próximo à Roseta, cerca de 56 km ao leste de Alexandria, enquanto conduzia um grupo de engenheiros para o Forte Julien, o exército de Napoleão se deparou com um grande bloco de granito negro contendo, escritas sobre ele, o que parecia ser três textos em diferentes línguas, separadas em três partes distintas [2].

A mensagem escrita na pedra é um tipo de oração. Tais inscrições registram um decreto instituído em 196 a.C. sob o reinado de Ptolomeu V [3], escrito na realidade em duas línguas: Egípcio Tardio e Grego. A parte da língua egípcia foi escrita em duas versões, hieróglifos e demótico[1]; sendo esta última uma variante cursiva da escrita hieroglífica. O faraó Ptolomeu V havia concedido ao povo a isenção de uma série de impostos e o fato, evidentemente, alegrara a todos. Em sinal de agradecimento, os sacerdotes resolveram erguer uma estátua de Ptolomeu V em cada templo e organizar festividades anuais em sua honra. Estelas comemorativas foram construídas e colocadas em cada templo importante da época. Foi uma dessas pedras que os soldados de Napoleão se depararam. Apesar de estar mutilada, foi possível reconstituir a totalidade do texto original graças a outras cópias do decreto encontradas posteriormente [2].

Levada a Europa, a pedra começa a ser estudada por acadêmicos. Houve a hipótese de que os três textos fossem o mesmo, mas apenas o grego podia ser entendido. Qualquer conhecimento sobre a escrita em hieróglifos havia sido perdido desde o século IV a.C., e do demótico pouco depois [2]. Como o grego era uma língua bem conhecida, a pedra poderia servir como chave para a decifração dos hieróglifos.

[1] O alfabeto “demótico” foi um tipo de escrita popular, adotado pelas classes mais pobres da sociedade egípcia. O termo “demótico” provém do grego “demotika”, que significa “popular” ou relativo aos assuntos diários.

O principal desses estudiosos chamava-se Thomas Young[2] (1773 – 1829). Ao longo de vinte anos de trabalho, Young conseguiu traduzir consideráveis porções do texto da Pedra da Roseta [4]. Ele foi a primeira pessoa desde a queda do Império Romano a poder ler um texto demótico e apesar de alguns erros cometidos, ele mereceu ser conhecido como o decifrador do demótico [3]. Mas o interesse de Young morrera e o personagem que daria continuidade a essa história seria o jovem Jean-François Champollion (1790 – 1832), um daqueles exemplos de gênios precoces que logo cedo demonstrou talento no estudo de línguas [5].

No outono de 1821 o obelisco que tinha sido adquirido por um amigo de Young, William Bankes, chegara à Inglaterra[6]. O texto contido em tal obelisco também era bilíngüe com campos em grego e em hieróglifo. A inscrição mencionava o nome de Cleópatra e não foi difícil identificá-lo. O mesmo aconteceu com o nome de Ptolomeu na Pedra da Roseta [7]. Isso não passou despercebido por Champollion e no dia 27 de setembro de 1822, ele apresentou suas descobertas diante da ***Académie dês Inscriptions et Belles Lettes***. Ele havia esboçado o alfabeto hieroglífico isolado com sucesso na Pedra da Roseta e no obelisco de Bankes [8].

1.1 O Método

Ao estudar a Pedra de Roseta, Champollion identificou o único cartucho que aparecia seis vezes como sendo o de Ptolomeu, dado que a secção grega referia que a inscrição era sobre um Ptolomeu. Ele assumiu que os caracteres seriam a pronunciação de Ptolemaios, a palavra grega para Ptolomeu (FIGURA 1.1).

FIGURA 1.1: Cartucho egípcio representando Ptolomeu V encontrado na Pedra da Roseta. (Fonte: http://hieroglifos.com.sapo.pt/champollion.htm)[3]

[2] O mesmo do experimento da dupla fenda da óptica e do módulo de Young da mecânica. Ele não se destacou apenas na física, mas em trabalhos em anatomia, onde foi revolucionário em pesquisas sobre o olho humano e seus defeitos, e foi um apaixonado pelo estudo das linguagens [2].

[3] As demais figuras desta secção foram retiradas da mesma fonte.

No obelisco de Bankes, encontram-se dois nomes reais na secção grega: Ptolomeu (**Ptolemaios**) e Cleópatra (**Kleopatra**). No texto hieroglífico dois cartuchos aparecem lado a lado. Um deles é quase idêntico ao da Pedra de Roseta (Figura 1.2).

FIGURA 1.2: Cartucho egípcio representando Ptolomeu V encontrado no obelisco de Bankes.

Outro cartucho, no Obelisco de Bankes, foi identificado como sendo o nome de Cleópatra (Figura 1.3).

FIGURA 1.3: Cartucho egípcio representando Cleópatra, também encontrado no obelisco de Bankes.

Assim, decompondo os cartuchos de Ptolomeu e Cleópatra, temos os seguintes hieróglifos:

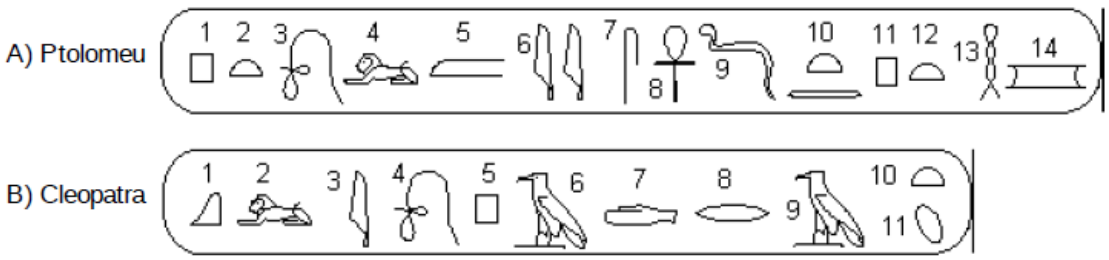


FIGURA 1.4: Indicação dos hieróglifos nos cartuchos egípcios representando Ptolomeu (A) e Cleópatra (B), também encontrados no obelisco de Bankes.

Champollion concluiu que A1 = B5, logo, deveria representar a letra P. De modo análogo, A4=B2 e deveria representar L. Concluiu também que B1 deveria ser K. Os sinais B3 e B4 devem ser provavelmente os equivalentes às vogais *E* e *O*, respectivamente. Em algumas formas do cartucho de Cleópatra, o sinal B7 é substituído por B10, que é o mesmo que A2. Provavelmente ambos significam *T*. B6 e B9 devem ser *A*. Temos então:

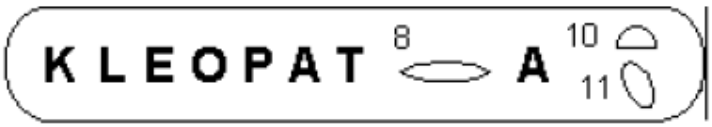


FIGURA 1.5: Substituição dos símbolos, no hieróglifo representando o nome de Cleópatra, pelas letras correspondentes as letras E, O, A e T.

Os últimos dois sinais (B10 e B11) já eram conhecidos desde os estudos de Thomas Young como sendo uma terminação honorífica em nomes de deusas, rainhas e princesas. Ou seja, não teriam valor fonético. Isto faz com que B8 = ***R***. Assim, substituindo agora as letras conhecidas no cartucho de Ptolomeu:

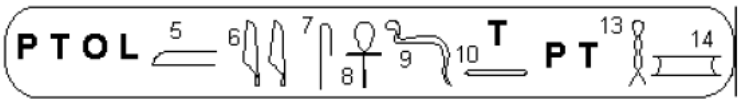


FIGURA 1.6: Substituição dos símbolos, já decodificados, no hieróglifo representando o nome de Ptolomeu.

Verifica-se que alguns sinais não correspondem a nenhuma parte do nome (em grego **Ptolemaios**). Mas existem outras formas de Ptolomeu na Pedra de Roseta, e Champollion comparou-as (FIGURA 1.7):

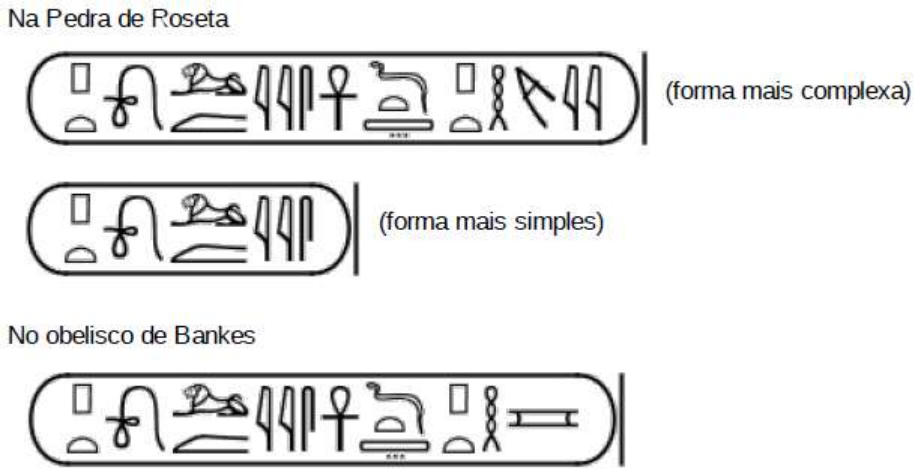
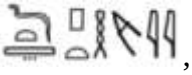


FIGURA 1.7: Comparação entre os cartuchos com o nome de Ptolomeu encontrado na Pedra da Roseta e no Obelisco de Bankes.

Os últimos hieróglifos, a saber  e  , nos cartuchos maiores, deveriam corresponder aos ***epítetos reais*** mencionados no texto grego, ***"viva para sempre, o amado de Ptah"***. Deveriam por isso ser equivalentes entre si. O último hieróglifo, na forma mais simples do cartucho de Ptolomeu, deveria ser o S de **Ptolemaios**. Os sinais restantes,  e  , podiam traduzir-se como ***M*** e uma vogal semelhante a ***I***. Champollion

tinha descoberto o segredo: a antiga escrita hieroglífica egípcia era uma mistura de sinais representando sons (***fonogramas***) com sinais que representavam idéias ou palavras (***ideogramas*** ou ***logogramas***).

O método aqui exposto foi encontrado num **site** sem referência alguma sobre o autor ou sobre sua fonte de pesquisa. No entanto, correto ou não, ele é nosso primeiro exemplo de um método de ataque criptográfico a uma mensagem desconhecida. Em outras palavras, é a tentativa de se entender um texto cujo conteúdo esteja protegido, intencionalmente ou não (como é o presente caso), por algum modo de codificação, impedindo o leitor de acessá-lo diretamente sem o conhecimento de um modo de traduzi-lo, de decodificá-lo.

1.2 Teoria Criptográfica: Conceitos Básicos

Na maior parte da história humana, o problema de se decodificar uma mensagem expressa numa linguagem desconhecida não se deu sempre de forma acidental, como decorrência do completo ocaso de uma cultura. É bem verdade que nas discussões sobre criptografia o tema relacionado ao resgate de culturas primitivas cujo conhecimento de suas línguas perdeu-se no tempo, como no caso dos hieróglifos egípcios já citados, sempre antecede qualquer outra discussão[4]. Entretanto, pelo menos nos últimos três mil anos, pessoas

[4] O mesmo problema ocorreu de forma semelhante com outras culturas antigas, entretanto nem em todas elas a decodificação foi tão bem sucedida. É possível citar rapidamente três outros exemplos bastante interessantes. Uma civilização desenvolveu-se na ilha de Creta entre 3000 a.C e 1100 a.C. O único vestígio restante de sua escrita é um disco de argila de aproximadamente 16 cm de diâmetro chamado *Disco de Festos*, descoberto em 1908 contendo um total de 242 símbolos. O problema de se achar o significado desses símbolos é que ele é único e que não há outros textos na mesma escrita. É o mais curto dos textos existentes e não temos dicas suficientes para obter resultados com métodos estatísticos. Até hoje ninguém foi capaz de decodificá-la [9]. O segundo exemplo vem da civilização Maia que viveu por volta de 2000 a.C. a 1500 a.C.. Os Maias possuíam talvez uma das mais difíceis linguagens de ser decifradas: são os hieróglifos Maias. São mais de 800 símbolos que, na maioria, representam os mais diversos objetos. Até a metade do século vinte, quase nada havia sido decifrado. Apenas do meio para o fim do século houve um avanço significativo nas traduções. Entretanto, uma quantidade muito grande de material ainda precisa ser decifrado [10]. O terceiro exemplo é talvez aquele mais envolto em mistério. Trata-se da linguagem usada pelo povo que viveu na ilha de Páscoa, a ilha mais a leste das ilhas polinésias, famosas por suas grandes cabeças de pedra. Vários tabletes foram encontrados com uma língua chamada Rongorongo. Existem ao todo 120 símbolos combinados em grupos de três para formar palavras. A decodificação dessa língua pode selar a solução dos principais mistérios que envolvem a ilha de Páscoa, mas apenas pouco mais de trinta fragmentos restaram. Muitos dos tabletes foram destruídos pelos primeiros missionários cristãos por se tratar de elementos de culto pagão. A quantidade de texto restante é muito pouca para análise. Para piorar, o

desejaram enviar mensagens que deveriam ser lidas apenas por outras a quem tais mensagens fossem designadas. Quando a mensagem é enviada por um mensageiro até o receptor (um escravo, como na Antiga Grécia ou Roma, por exemplo) ou pelos correios dos dias atuais, há um risco de desvio (o escravo pode ser capturado ou o carteiro pode entregar a correspondência num endereço errado). Se a mensagem for escrita claramente, ou seja, numa linguagem natural, qualquer pessoa que tiver contato com a mesma está habilitada a lê-la e entender seu conteúdo. Isso consiste um problema de suma importância num campo de batalha, por exemplo.

Os espartanos foram os primeiros a fazer uso da criptografia em questões bélicas. Eles usavam um dispositivo de transposição de cifra primitivo bastante interessante. Era constituído de um bastão (FIGURA 1.8), um cilindro, com uma tira de couro em volta dele sobre o qual era escrita a mensagem. O receptor da mensagem usava uma vara de mesmo diâmetro no qual ele punha em volta a tira de couro para ler a mensagem. Era um método prático, rápido e não estava suscetível a erros na decodificação, algo fundamental num campo de batalha [12].

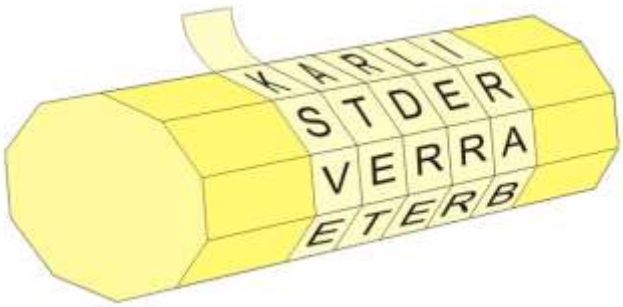


FIGURA 1.8: Bastão espartano usado para a criptografia de mensagens de guerra.

O código, contudo, era fácil de ser quebrado uma vez que a tira de couro com a mensagem já oferece um bom indício. Funcionava da seguinte maneira: suponha que a mensagem que se desejava enviar era “estamos sendo atacados”. Tais letras dispostas em uma tira de couro seriam: “EODC SSOA TSAD AETO MNAS”. Mas quando a tira fosse envolvida no bastão a imagem formada em cada linha pode ser comparada a FIGURA 1.9, abaixo. O uso de um dispositivo como esse tem sido datado de algo em torno de 475 a.C..

Rongorongo não tem parentes próximos na face da Terra para permitir uma análise comparativa [11].

	E	S	T	A	M	
	O	S	S	E	N	
	D	O	A	T	A	
	C	A	D	O	S	

FIGURA 1.9: Exemplo de uma mensagem criptografada com um bastão espartano.

Mais crédito vem dos gregos em termos do desenvolvimento dos primeiros métodos de substituição. Políbio (200 – 180 a.C.) inventou um meio de codificar letras num par de números. O método pode ser acompanhado fazendo uso da TABELA 1.1, chamada ***Quadrado de Políbio***.

TABELA 1.1: Quadrado de Políbio.

	1	2	3	4	5
1	a	b	c	d	e
2	f	g	h	ij	k
3	l	m	n	o	p
4	q	r	s	t	u
5	v	w	x	y	z

Fonte: Referência 12.

Aqui, as letras “i” e “j” foram consideradas uma única letra[5]. Cada letra é a intersecção de uma linha com uma coluna. Se tomarmos a letra “b”, por exemplo, ela seria representada por 12. A “m” por 32 e assim por diante. Dessa forma, as letras são o ***texto comum*** e os números o ***texto cifrado***[6].

1.2.1 Criptografia e Criptoanálise

[5] Muito provavelmente isso ocorria no alfabeto grego, uma vez que nele existem 31 letras ao todo.

[6] Na Antiguidade, esse método era usado para enviar mensagens com tochas em cima de colinas. O mensageiro tinha uma tocha em cada mão e acenava com a mão direita o numero de vezes equivalente a linha e com a esquerda o equivalente a coluna. Das variantes desse sistema, a mais interessante foi desenvolvida por prisioneiros Russos, no século vinte, transforamando os dígitos em números de batidas, podendo assim conversar entre sí estando em celas separadas [11]. Os trechos acima citados são apenas uma pequena amostra de como a criptografia esteve presente ao longo da História de diversas culturas. Falar sobre a contribuição dos árabes, dos chineses, dos indianos e de tantas outras culturas antigas preencheriam várias páginas com exemplos dos mais diversos. Um leitor interessado pode facilmente encontrá-los numa vasta literatura sobre a história da criptografia [10, 11].

Atualmente, mensagens são enviadas por via rádio, sinais de TV, fax, e-mail, etc., e a possibilidade de serem interceptadas não só ainda está presente como tem crescido. De um lado, há aqueles que desejam proteger tais mensagens, do outro, aqueles que precisam descobrir seu conteúdo. O esforço requerido por um rival, oponente ou inimigo para ler a mensagem sempre se mostrou relevante.

É nesse amplo contexto que, antes de discutirmos o problema principal ao qual concerne este trabalho, ou seja, a criptografia em sistemas ópticos, torna-se lícito entendermos a evolução dos modelos e métodos usados por aqueles que desejavam esconder informações e daqueles que desejavam descobri-las a todo custo. Entramos, portanto, no campo da criptologia.

A *criptologia* é a ciência que trata com métodos para prover segurança no armazenamento e transporte de informações no seu sentido mais amplo. O nome criptologia é uma combinação do grego kryptos, que significa escondido, e logos, que significa estudo, ciência. Em outras palavras, tal ciência é constituída de métodos para *codificar* mensagens e sinais, assim como métodos para *decodificá-los* [13].

A criptologia pode ser dividida em duas partes: *criptografia* e *criptoanálise*[7][12,14]. A *criptografia* pode ser definida como a área da criptologia que trata com técnicas baseadas em uma *chave secreta* para ocultar ou *cifrar* dados. Em princípio, apenas aquele que tem acesso a chave é capaz de decifrar a informação criptografada. A primeira parte da palavra criptografia deriva também de kryptos e a segunda parte vem de graphien, que significa escrever [12]. A criptoanálise, por sua vez, trata com técnicas para decifrar dados criptografados sem o conhecimento da chave usada. Mais precisamente, a criptoanálise é a ciência matemática que trata com a análise de sistemas criptográficos para obter conhecimento necessário para quebrar o código que protege a mensagem, ou contornar tal proteção. É evidente que criptografia e criptoanálise estão fortemente relacionadas [13].

[7] É possível encontrar na literatura a inclusão do termo *estenografia* a esta lista. A palavra vem do grego *steganos*, que quer dizer impenetrável. Assim a palavra pode ser entendida como "escrita impenetrável". Ela refere-se a métodos de esconder a existência de mensagens ou outros dados com a diferença que a estenografia tenta esconder a própria mensagem e não apenas o seu significado. Um exemplo moderno são os métodos de esconder arquivos eletrônicos.

Algoritmo criptográfico é um algoritmo[8] que emprega e faz uso de técnicas criptográficas e seus mecanismos. *Protocolo criptográfico* é um protocolo que emprega e faz uso de técnicas criptográficas e seus mecanismos [14]. *Criptossistema* é um conjunto de algoritmos criptográficos que inclui algoritmos para a geração de um par de chaves para codificação e decodificação [15]. É possível apreciarmos uma definição mais matemática. Um criptossistema (ou *esquema de codificação criptográfica*) é uma tupla (*P, C, K, E, D*) onde *P* é o espaço dos textos comuns, *C* é o espaço dos textos cifrados e *K* é o espaço das chaves. $E = \{E_k : k \in K\}$ é uma família de funções $E_k : P \rightarrow C$. Seus elementos são chamados *funções de codificação criptográfica*. $D = \{D_k : k \in K\}$ é uma família de funções $D_k : C \rightarrow P$. Seus elementos são chamados *funções de decodificação criptográfica*. A definição se completa quando para cada $e \in K$, existe um $d \in K$ tal que $D_d(E_e(p)) = p$ para todo $p \in P$ [16].

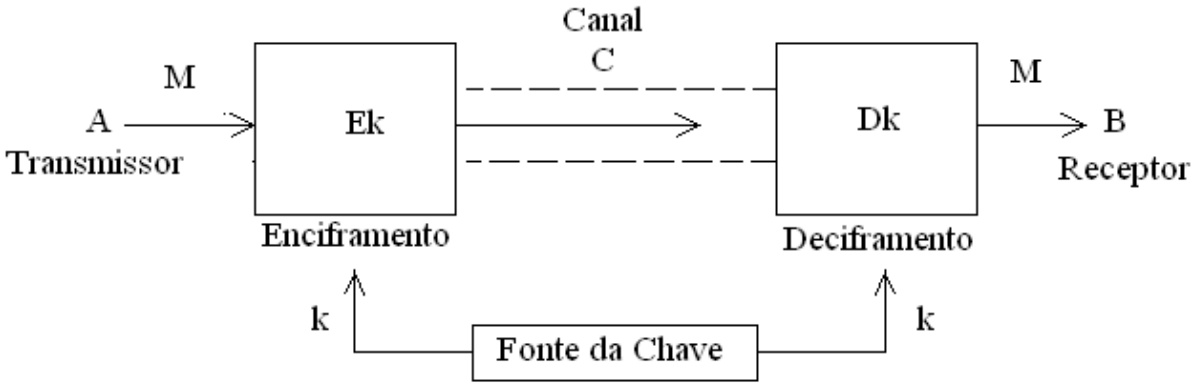


FIGURA 1.10: **Esquema básico de criptografia de uma mensagem M enviada com segurança por um canal C.**

A primeira impressão de um algoritmo criptográfico é visto na seguinte situação (FIGURA 1.10). Suponha que A (o transmissor da informação) deseja enviar uma mensagem criptografada, ou seja, um código secreto, para B (o receptor da informação). Seja M o texto principal (chamado de *texto comum*) e C o *texto cifrado*. Um possível método é usar uma *chave k* para criptografar M [17].

O transmissor A deseja mandar uma mensagem ao receptor B e deseja, além disso, que apenas B tenha conhecimento do conteúdo da mensagem. A usa então uma *chave k* para, através de um método a escolha de A, codificar a mensagem M e assim poder enviá-la através do canal C. O canal C não é necessariamente um canal seguro e um terceiro pode tentar interceptar a mensagem enviada por A. Através de um meio, também à escolha de A, a chave é entregue a B e este, e apenas este, poderá decodificar a mensagem, uma vez que qualquer intruso que venha interceptar a mensagem não tem conhecimento da chave.

1.2.2 Objetivos da Criptografia

A confidencialidade não é o único objetivo da criptografia. Ela também é usada para solucionar outros problemas. O primeiro deles é o da *integridade de dados*. O receptor deve estar hábil a checar se a mensagem foi modificada durante a transmissão, seja acidentalmente ou deliberadamente. Não deve ser permitido a ninguém substituir a mensagem real, ou parte dela, por uma falsa. Outro problema é o da *autenticação*. O receptor da mensagem deve estar hábil a verificar a origem da mensagem recebida. Por último, há o problema da *não-repudiação*. Quem envia a mensagem não deve poder negar tê-la enviado [13].

Métodos de *chaves simétricas* e *chaves públicas*[9] [18, 19] que garantem a integridade das mensagens. Classicamente, métodos simétricos requerem uma chave secreta *k* compartilhada entre aquele que envia a mensagem e aquele que a recebe. A mensagem é acrescida de uma *mensagem código de autenticidade*. Tal código é gerado por um algoritmo que depende de uma chave secreta [13, 16, 17, 20].

O criptógrafo holandês Kerkhoff (1835-1903) foi o primeiro a formular a *regra para a segurança de codificação*, na qual o mecanismo de codificação completo é conhecido pelo oponente e a segurança do algoritmo pode apenas ser determinado pelo valor conhecido da chave secreta. Isto significa que um oponente não tem como quebrar a proteção, ou encontrar

---

[8] Por mera formalidade, apresentaremos a definição de algoritmo: um algoritmo é um procedimento computacional bem definido que recebe uma variável de entrada e gera uma correspondente variável de saída.

[9] Seremos mais específicos quanto a esses termos em outro momento.

a verdadeira chave em um tempo significativamente menor que o tempo que levaria pra tentar todas as chaves secretas possíveis [21].

1.2.3 Ataques Criptográficos

A criptoanálise moderna parte do pressuposto que o invasor conhece qual o criptossistema que está sendo usado. É pressuposto que apenas a chave (privada) e o texto comum são secretos. O invasor tenta recuperar os textos comuns a partir dos textos cifrados ou tenta descobrir quais chaves estão sendo usadas.

Um ataque somente ao texto cifrado consiste na decodificação criptográfica do texto cifrado usando todas as chaves possíveis. Esse ataque é chamado de *busca exaustiva*. Dada a velocidade dos computadores modernos, esse tipo de ataque é bem-sucedido sobre muitos criptossistemas. Ele funciona, por exemplo, para o Data Encryption Standard (DES) que até recentemente era o padrão de codificação criptográfica nos Estados Unidos [16,22,23]. Podem-se definir basicamente três situações:

a) o criptoanalista tem apenas os textos cifrados;
b) o criptoanalista tem os textos cifrados e os textos comuns;
c) tem os textos cifrados e os comuns para um texto que ele próprio escolheu.

A primeira situação é obviamente aquela que poderíamos chamar de normal. A segunda situação pode surgir, por exemplo, se mensagens idênticas são enviadas ambas usando a nova cifra e usando uma “velha” cifra que o criptoanalista pode ler. Tais situações constituem uma séria quebra da segurança, o que ocorre não com pouca freqüência. A terceira situação surge principalmente quando o criptoanalista, desejando testar a força do seu sistema, desafia colegas a agir como inimigos para resolver o sistema. É um procedimento padrão em novos sistemas. Um sistema de codificação que não possa ser resolvido mesmo na terceira situação é um realmente forte [16].

Quando um criptoanalista vê uma mensagem cifrada, seu primeiro problema é descobrir que tipo de sistema de codificação foi utilizado. Para fazer isto, ele primeiro leva em conta qualquer informação colateral disponível[10]. Analisa o preâmbulo da mensagem, onde deve conter informações sobre o receptor, a quem a mensagem foi intencionada e analisa também a própria mensagem. Se muito curta, é praticamente impossível fazer grandes progressos e deve esperar por novas mensagens. Se longa o suficiente, ou se ele já tem obtido um bom número de longas mensagens, ele deveria aplicar uma variedade de testes matemáticos que poderia certamente dizê-lo se foi usado um código simples, um sofisticado, ou um conjunto deles. Identificado o sistema, o criptoanalista deve poder estimar quanto material (ou seja, quantas letras cifradas) ele necessitará para ter uma razoável chance de quebrar o código.

1.3 Sistemas Criptográficos Clássicos

1.3.1 O Código de César

Praticamente todos os sistemas criptográficos clássicos surgiram em auxílio direto ou muito próximo a questões militares. O ***código de César*** foi o primeiro código a ter um sério uso militar. Seu propósito era permitir a passagem de informação entre comandantes com algum grau de segurança [24].

Antes de apresentarmos a idéia básica por trás do código de César, usaremos a oportunidade para distinguir dois tipos de sistemas clássicos de criptografia: ***sistemas de transposição*** e ***sistemas de substituição*** [13]. Os sistemas de transposição estão baseados na mudança na seqüência de caracteres em um texto comum. Os próprios caracteres permanecem inalterados. Os de substituição, por sua vez, não alteram a ordem dos caracteres no texto comum, mas troca os originais por outros.

Podemos apreciar com mais detalhes um sistema de transposição no exemplo a seguir.

[10] Um exemplo disso são os padrões idiomáticos que podem transparecer mesmo após a criptografia, e que veremos com detalhes mais a frente.

***Texto comum**:* ESTAMOS SENDO ATACADOS
***Blocos**:* ESTAM OSSEN DOATA CADOS
***Texto cifrado**:* AMTES ENSOS TAADO OSDCA

O texto comum é dividido em blocos de cinco letras. Podemos dizer que o período aqui é igual a cinco. Cada bloco foi então reorganizado de acordo com a chave 4 5 3 1 2, onde estamos considerando cada número como a ordem original no bloco. Muitas vezes associa-se a essa mudança uma palavra para lembrar-se facilmente a ordem e é chamada de ***palavra-chave*** [13].

Considere uma mensagem M com um comprimento total L = *n*T letras, onde T é o período e *n* um inteiro positivo. Os criptoanalistas se deparam com dois problemas. O primeiro é encontrar o período T que implicam em tentar todas as combinações de *n* e T, que satisfaz L = *n*T, com L igual ao comprimento da mensagem. O segundo problema é encontrar a própria chave sem necessariamente tentar todas as possíveis permutações.

Para resolver esses problemas, o criptoanalista pode beneficiar-se das características da língua na qual o texto comum é escrito. Certas letras, por exemplo, são mais freqüentemente usadas em um dado idioma que outras [13]. Na língua portuguesa, a letra que mais aparece em um texto é a letra *a*. As vogais em geral aparecem com muito mais freqüência na maioria dos idiomas.

Os sistemas de substituição são baseados na troca de caracteres do texto comum com outros caracteres. Assumindo que o texto comum seja baseado em um alfabeto de 26 letras, uma cifra de substituição pode ser descrita pelo seguinte:

Alfabeto do texto comum: A = [a_1, ..., a_{26}]
Alfabeto do texto cifrado: B = [b_1, ..., b_{26}]
Texto comum: a_3, a_{23}, a_9, a_{17}, a_4
Texto cifrado: b_3, b_{23}, b_9, b_{17}, b_4

Esta é a mais fácil cifra de substituição, é a substituição de César, ou código de César. O alfabeto de substituição é obtido pela simples mudança do alfabeto original por um dado número de caracteres, com respeito ao alfabeto original. Se os caracteres dos textos comum e

cifrado forem numerados e denotados por i e j respectivamente, supondo uma mudança de três lugares, para todo $i = 1, ..., 26$: $j = i + 3$ (módulo 26). Numa forma mais geral, $j = i + t$ (módulo 26), no qual t representa o número de caracteres a ser mudado de lugar no alfabeto.

Uma importante característica no código de César é que a ordem dos caracteres do alfabeto de substituição permanece inalterada. O número total de chaves não deve exceder 26, de tal forma que é muito fácil quebrar o código. Se a mensagem for suficientemente longa, tornar-se-á mais fácil ainda. Basta observarmos que a letra que mais ocorre é a letra que mais ocorre no alfabeto original. Podemos tentar aprimorar o modelo inserindo símbolos distintos para as pontuações e mesmo para os espaços, mas mesmo essas medidas tornam o método ainda muito ingênuo. Uma forma mais eficiente de aprimorar o método de César é fazer a troca de letras randômicam. Assim, o número de chaves aumentaria para 26! Isso tornaria o deciframento mais difícil [14].

Em geral, os métodos de substituição não são muito resistentes a ataques, uma vez que características da linguagem podem ainda ser extraídas do ***texto cifrado***. Isto pode ser evitado aplicando mais de uma cifra de substituição. Tal procedimento é chamado de ***substituição polialfabética***, oposta a ***substituição monoalfabética*** exemplificada anteriormente. Um exemplo bem conhecido de substituição polialfabética é o ***sistema de Vigenère***, elaborado em 1568 pelo francês Blaise de Vigenère. Tal sistema usa uma diferente substituição de César para cada letra [14].

Tabela 1.2: Tabela de Vigenère.

	A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

A codificação baseada no sistema de Vigenère é geralmente realizada com a ajuda da ***tabela de Vigenère*** e uma palavra chave. A primeira linha da tabela de Vigenère consiste de letras do alfabeto do texto comum e a primeira coluna contém letras da palavra-chave. Um texto pode ser cifrado usando o seguinte procedimento.

A palavra-chave é repetida abaixo do texto comum, como no exemplo abaixo. A letra do texto criptografado é igual à letra localizada na intersecção da coluna designada pela letra do texto comum e a linha designada pela letra da chave.

Texto comum: ESTAMOS SENDO ATACADOS
Chave: CHAVECH AVECH AVECHAVE
Texto cifrado: GZTVQQZ SZRFV AOEEHDJW

Uma dada letra no texto comum é representada por diferentes letras no texto cifrado, dependendo da letra da palavra chave, cancelando assim as características lingüísticas mais eficientemente que qualquer outro método. O número de substituições monoalfabéticas no qual o sistema de Vigenère é baseado é igual ao comprimento da palavra chave. No nosso exemplo, cinco. Obviamente se o criptoanalista puder descobrir o comprimento da palavra-chave, tal conhecimento será de grande importância para encontrar a solução do criptograma.

1.3.2 One-Time Pad

Sempre com o surgimento de um método criptográfico, surge também uma corrida para a quebra do mesmo, uma vez que estamos falando basicamente da segurança de estados. O método de Vigenère teve seu êxito comprovado por muitos anos até finalmente ser quebrado. O ataque Babbage/Kasiski é um método de ataque a cifras de substituição polialfabética e mostrou ser eficiente contra o método de Vigenère.

Tal método permite descobrir o comprimento da chave usada. Uma vez que tal comprimento é descoberto, as colunas do texto cifrado são atacadas sistematicamente. O método de Babbage/Kasiski é difícil de ser realizado manualmente, mas chegava as mãos dos criptoanalistas uma ferramenta primordial: o computador. Este era capaz de fazer os cálculos necessários em pouco tempo de tal forma que a quebra do código de Vigenère era uma realidade[11].

A quebra do criptossistema Vigenère trouxe a necessidade do desenvolvimento de novos, mais fortes e eficientes criptossistemas. Seria possível então conceber um código tão forte que seja absolutamente inquebrável? A fraqueza do código de Vigenère encontra-se na palavra chave sendo curta e reconhecível. Mas quão longa deve ser tal chave para impedir tal processo? A resposta foi dada em 1918 por Gilbert S.Vernam. Vernam (1890-1960) foi um criptologista da AT&T. Ele percebeu que se o código Vigenère fosse usado com uma chave randômica, com ***comprimento de chave*** do tamanho do ***texto comum***, então a ataque Babbage/Kasiski falharia. Para fazê-la irreconhecível, fazemos a palavra chave completamente randômica. A AT&T trabalhava estritamente com as forças armadas, de tal

[11] Uma forma completa do funcionamento do ataque de Babbage/Kasiski pode ser encontrada em [15,12,17,26,27].

forma que a companhia reportou isso ao exército. Tal descoberta chamou a atenção do Major Mauborgne que acrescentou a seguinte idéia: ***a chave deveria ser usada uma única vez e depois ser descartada***. Tal sistema é chamado ***one-time pad*** (ou cifra de *Vernam*). Uma vez que a chave seja tão longa quanto o texto comum e a chave selecionada sendo randômica e usada exatamente uma vez, então o texto cifrado será realmente randômico. Assim, ***o one-time pad é inquebrável*** [11, 12, 14].

Quem envia e quem recebe a mensagem nesse sistema, necessita de uma cópia idêntica do ***one-time pad***, que consiste de não mais que uma longa e totalmente randômica cadeia de caracteres do alfabeto. Apenas eles possuem essa super chave. A mensagem secreta é então enviada em qualquer meio conveniente. Uma vez que a palavra chave nunca termina (ou mais precisamente, não termina enquanto a mensagem não for concluída) não existe ciclo de cifras. Após a mensagem ser transmitida aquele que envia a mensagem destrói a chave assim como faz o receptor. Embora custoso, esse método é seguro. Se a mensagem cifrada é interceptada durante a transmissão, ela é de pouco uso para o interceptador não autorizado sem acesso ao ***one-time pad***.

Em princípio, todos os aspectos da mensagem podem ser escritos na forma de códigos binários e a mensagem torna-se uma grande cadeia consistindo de símbolos 0 e 1. Se o dígito da mensagem fosse ***a***, e o dígito randômico na cadeia correspondente fosse ***b***, então a mensagem transmitida seria ***a+b***, onde a soma é calculada de acordo com as regras aritméticas de módulo 2. Por exemplo, se a mensagem fosse simplesmente uma cadeia do tipo 1111111, e os primeiros dígitos do ***one-time pad*** fossem 0111011, então a mensagem transmitida seria algo do tipo 1000100. O interceptador não autorizado terá acesso a uma cadeia randômica que não contem informação; que isoladamente, é sem significado.

Essa era a meta da criptografia! No entanto, perfeição tem o seu preço: há dois problemas distintos. Encontrar chaves realmente randômicas não é uma tarefa fácil. Mesmo computadores modernos não conseguem gerar chaves verdadeiramente randômicas. O melhor

que alguém pode esperar de computadores é que as chamadas ***pseudorandomicidades***, que é uma simulação de números randômicos. Isso por si só é um inteiro ramo de estudo[12] [25,26].

1.4 Chaves-Públicas

1.4.1 Princípio dos Criptossistemas de Chave-Pública

Novos desenvolvimentos forçaram o ajuste de como os códigos de segurança seriam utilizados. Na **internet**, por exemplo, é muito diferente do uso tradicional. Quando um cliente envia informações pessoais pela **internet**, como o número do cartão de crédito, por exemplo, ele precisa estar seguro que tal informação não será interceptada e transferida para outro lugar. A transferência segura é realizada efetivamente através da informação sendo codificada. O usuário não sabe nada dessa codificação ou como ela é feita. Isto é realizado automaticamente sem o conhecimento do cliente. Existe potencialmente um grande problema com isso. A codificação tem que ser feita antes da transmissão, de outra forma não há segurança. É assim que a codificação ocorre no domínio público. Se uma parte inescrupulosa toma acesso às transmissões codificadas, e também sabe como cifrar a mensagem, seguramente não será tão difícil reverter o processo e decifrar a mensagem original. Isso poderia ser desastroso e fazer com que tal transação seja insegura.

Era preciso elaborar um código que podia estar no domínio público de tal forma que qualquer um pudesse usá-lo e enviar suas mensagens, mas, de alguma forma, tal pessoa seria

---

[12] Em meio ao surgimento de toda uma tecnologia que culminaria em modernos computadores com avançadíssima capacidade de vasculhar sistemas criptográficos, é bastante interessante destacar um fato curioso inicialmente ocorrido durante os últimos anos da primeira grande guerra mundial. Foram usados pelos americanos oito índios da tribo Choctaw para enviar mensagens vitais através de sinais de comunicação inseguros em suas línguas nativas. As línguas nativas americanas são extremamente complexas, difíceis de aprender e certamente para os alemães seria quase impossível de aprender, de tal modo que foi um meio efetivo de "codificar" dados importantes. O método foi tão bem sucedido que durante a segunda guerra mundial, os americanos empregaram similarmente índios da tribo dos Navajos para transmitir mensagens importantes. Os inimigos nunca quebraram tal código [12].

a única passível de decifrar a mensagem codificada. A chave pública é aquela que pode trancar, mas não pode destrancar o vaso contendo seu segredo. Nenhum assim chamado ***criptosistema de chave pública*** seria possível até que a solução deste problema fosse encontrada.

1.4.2 A Função Trapdoor e o RSA

Nos anos 70, muitos estavam envolvidos com a invenção da função ***trapdoor*** (alçapão). Cada usuário necessitaria de uma função ***f*** que poderia ser em princípio disponível para qualquer um e que poderia calcular seu valor ***f(x)***. Contudo, o possuidor da função, conheceria algo de vital que permitiria decifrar e recuperar ***x*** do valor de ***f(x)***. Além disso, outras pessoas, muito embora conheçam a função ***f(x)***, não devem ser aptos a deduzir sequer pedaços de informação se eles tentarem [27].

Isto parecia um pedido muito alto. Entretanto, foi obtido por Clifford Cocks em 1973 [28]. Após ser introduzido à idéia de criptografia de chave pública, ele inventou um sistema em torno de uma hora! Ele usou seus conhecimentos em ***teoria dos números*** para criar uma ***função alçapão*** com a requerida propriedade: dado ***x***, é possível calcular ***f(x)***, mas dado ***f(x)***, seja quase impossível recuperar o número ***x*** a menos que se conheça o segredo de sua estrutura. Este método é a base da criptografia pública usada hoje. Infelizmente, Cock trabalhou para uma organização governamental secreta de tal forma que sua grande descoberta nunca foi realizada no domínio público. As mesmas idéias foram dar com meia dúzia de matemáticos e cientistas da computação trabalhando nos Estados Unidos poucos anos depois. Os nomes geralmente associados à descoberta e ao desenvolvimento de criptografia de chaves públicas são Diffie, Hellman e Merkle junto com Rivest, Shamir e Adleman dos quais deriva a sigla dos códigos RSA. Hoje, o programa RSA é o pedaço de software mais utilizado na Terra [29].

O sistema RSA é baseado no fato de que é relativamente fácil calcular o produto de dois números primos, mas determinar os números primos originais, dado o produto, é de longe muito mais complicado. Suponha dois números primos cujo produto é n (n = pq). Então um número e é determinado satisfazendo a seguinte expressão:

$$3 < e < (p - 1)(q - 1) \qquad (1.4.1)$$

e que é relativamente primo à (p – 1)(q – 1). Em outras palavras, a maior fator comum de *e* e (p – 1)(q – 1) é 1. Finalmente o valor de *e* é usado para determinar outro número, *d*, para o qual:

$$ed = 1 \pmod{(p-1)(q-1)}. \quad (1.4.2)$$

A chave publica consiste do um par (*e*,*n*); os outros valores são mantidos em segredo [9]. O texto é codificado como segue: uma representação binária do texto é usada e dividida em blocos denotados por M. A codificação do bloco C é realizada elevando o valor decimal de M para a potência *e* e tomando o resto da divisão por *n*:

$$C = M^e \pmod{n}. \quad (1.4.3)$$

O ***texto cifrado*** é decodificado de forma similar, mas agora *d* toma o lugar de *e*:

$$M = C^d \pmod{n}. \quad (1.4.4)$$

A segurança desse método permanece no fato que é quase impossível calcular o valor de *d* se apenas a chave pública (*e*,*n*) for conhecida. Para encontrar *d*, os valores de p e q devem ser conhecidos. Se apenas *n* é público, o criptoanalista deve determinar p e q dele. Se *n* for da ordem de 200 dígitos, levaria algo em torno de 30 milhões de anos para encontrar *d* com a tecnologia atual [13].

1.4.3 O Sistema DES

O alemão Host Feistel (1915-1990), emigrado para os Estados Unidos em 1934, é considerado um dos pioneiros da segurança publica para criptografia usada em larga escala. Trabalhava em uma agência do governo americano, mas devido sua nacionalidade, era sabotado pelas próprias forças americanas (NSA). Aconselhado a trabalhar na IBM, criou um criptossistema usado no ***banco de sistema IBM2984***, conhecido hoje como ***Alternative Encryption Technique***, o então chamado ***Lúcifer*** [10]. Esse criptossistema foi oficialmente anunciado em 1977 como **Data Encryption Standard** (DES). DES é um exemplo de ***codificador por blocos***. Basicamente, ele cifra blocos de dados de tamanhos específicos [44].

O DES possibilita a codificação de blocos de 64 bits de ***texto comum*** em blocos de 64 bits de ***texto cifrado*** fazendo uso de uma chave secreta. Ele realiza uma série de permutações sobre a cadeia de blocos e a codificação da mensagem (de tamanho arbitrário) é feito através de um modo de operação padronizado. A chave secreta também é formada por uma cadeia de 54 bits. Entretanto, nem todos são usados e é costume dizer que o DES usa chaves secretas de 56 bits [14].

DES foi usado com sucesso em bancos, comércio, indústrias, etc. até que, em 1993, M.J. Weiner apresentou uma eficiente busca de chave que poderia levar horas (naquele tempo) sobre uma máquina custando um milhão de dólares para uma busca exaustiva no espaço de chaves, também chamado ***ataque a força bruta***, que significava que todas as chaves possíveis são tentadas para ver qual está sendo usada [13, 30]. O comprimento de chave de 56 bits, usado pelo DES, foi tornando esse criptossistema cada vez mais frágil a ataques por métodos modernos. Naquele ano, um grupo chefiado por Paul Kocher desenvolveu um computador por um quarto de milhão de dólares que ele usou pra encontrar uma chave DES numa rotina de 56 horas. Seis meses depois o mesmo grupo conseguiu em 44 horas. Em agosto de 2000, o DES foi trocado por um novo criptossistema chamado ***Advanced Encryption Standard*** (AES), que permitiu chaves de 128, 192 e 256 bits.

1.4.4 Sistemas de Chaves-Públicas

Examinamos rapidamente métodos criptográficos que tratam com informações fazendo uso de uma única chave para o processo de codificação. O transmissor precisa da chave para codificar a informação e o receptor para decodificá-la. Um problema de suma importância é o de como garantir que ambas, mensagem e chave, sejam enviadas com segurança. Uma saída é enviar a chave por uma linha de transmissão diferente daquela usada para o *texto cifrado*.

Nos chamados *sistemas de chave-pública*, duas chaves são usadas. Uma para codificar o texto e outra para decodificar. Aquela que codifica é conhecida por todos. Um sistema que mantém uma das chaves em segredo e a outra pública é chamado de *sistema de codificação*

assimétrico. Um sistema baseado em uma única chave, como o DES, é chamado *sistema de codificação simétrico* [14, 31].

Como já era de se esperar, um aspecto importante nos sistemas de chave-pública são as funções *trapdoor*, já discutidas[13]. Dessa forma, um dos mais conhecidos sistemas de chave-pública é o RSA.

1.5 Controle de Chave

Um aspecto que nos falta discutir é a importância das chaves empregadas por esses algoritmos e métodos. Freqüentemente a chave deve ser mantida em segredo, uma vez que a segurança de muitos algoritmos criptográficos e métodos dependem da chave, não importa quão engenhoso seja o algoritmo. Em outras palavras, acessar a chave é praticamente acessar a informação. Essa verdade não vale somente para sistemas simétricos, mas para qualquer sistema baseado em chaves públicas e secretas.

Nosso principal foco aqui é a distribuição dessas chaves. O clássico problema para a distribuição de chave é indicado na FIGURA 1.11. A chave é distribuída por um canal seguro. O canal seguro não é usado para a transmissão direta da mensagem em *texto comum*. [14]

---

[13] As funções *trapdoor* é um tipo de função "*one-way*". Funções *one-way* são funções relativamente fáceis de calcular , mas o mesmo não sendo verdade para o cálculo de sua inversa. Assim, na literatura, encontramos as duas nomenclaturas tratando do mesmo problema.

[14] Como já citado, esse método é usado por militares, onde um portador é encarregado de levar a chave. O mesmo não seria facilmente utilizado aqui.

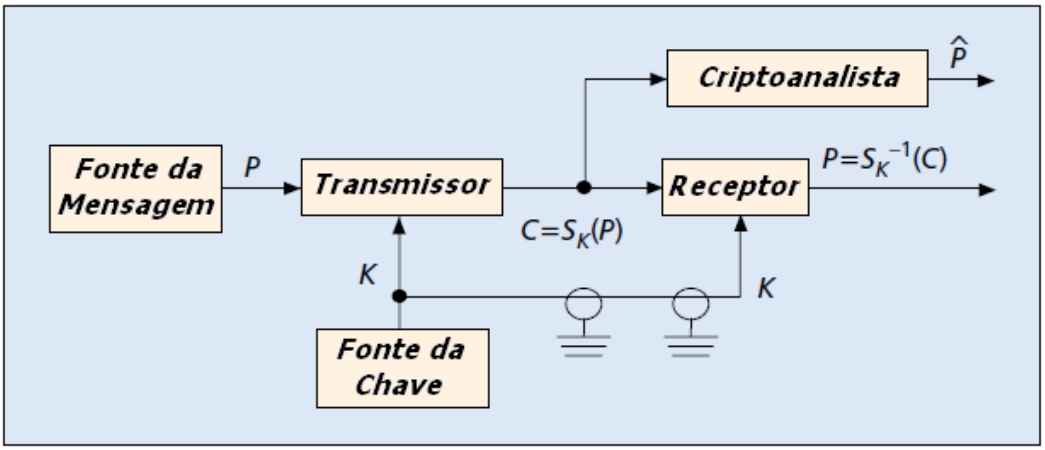


FIGURA 1.11: **Sistema criptográfico convencional.**

Diffie e Hellman [32] e independentemente Merkle [33] propuseram um forma radialmente diferente de resolver o problema da distribuição. Como indicado na FIGURA 1.12, uma comunicação segura toma lugar sem qualquer combinação prévia entre os participantes da conversa e sem acesso a um canal seguro de distribuição.

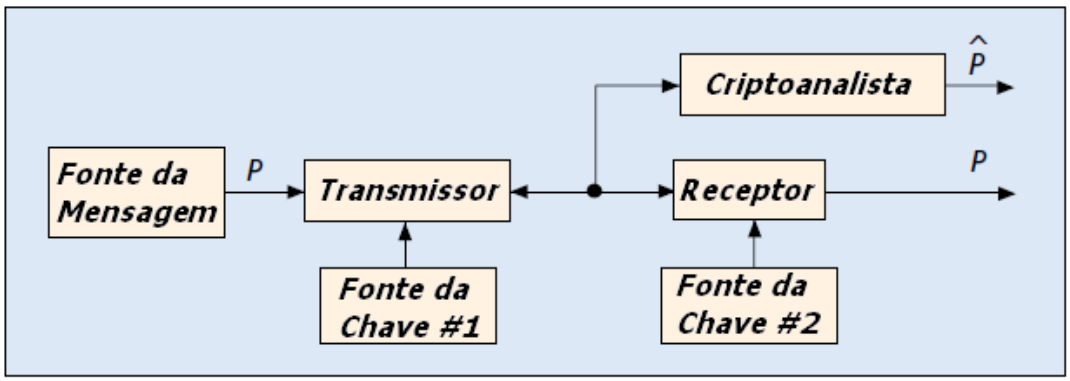


FIGURA 1.12: **Sistema criptográfico contendo dois canais de comunicação com geradores de números randômicos.**

Como indicado na figura acima, dois canais de comunicação são permitidos e há geradores de números randômicos independentes no transmissor e no receptor. Comunicações como essas são essenciais para distinguir o receptor autorizado do não autorizado. Do ponto de vista criptoanalítico, se houver ilimitado tempo computacional qualquer um quebrar o sistema, uma vez que, em tese, o criptoanalista pode tentar todas as chaves até ele encontrar uma que sirva. A questão real é se nós podemos, dadas as limitações computacionais, trocar

uma mensagem que, mesmo um criptoanalista com um poderoso computador, seja incapaz de compreender.

Os criptosistemas de chaves públicas têm duas chaves, uma para codificar e outra para decodificar. Enquanto as duas chaves efetuam operações inversas (e apesar de estarem relacionadas), não deve haver fáceis métodos computacionais que derivem uma chave da outra. A codificação pode ser feita pública sem comprometer a chave de decodificação de tal modo que qualquer um possa codificar mensagens, mas apenas o correto receptor as possa decifrar.

1.6 Conclusão

O sistema criptográfico que iremos propor evidentemente se apresentará num certo sentido um pouco distinto dos sistemas apresentados até aqui. A discussão que se apresentou visou apenas sistemas clássicos no intuito de introduzir o leitor aos conceitos básicos da criptografia. Diversas áreas de estudo se desenvolveram para auxiliara a testar a confiabilidade e a eficiência de um sistema assim como de um dispositivo criptográfico e não seria possível aqui nos debruçarmos sobre elas sem tornar o texto deste trabalho consideravelmente extenso.

Discussões sobre a melhor forma de como transportar ou armazenar chaves estão obviamente muito além daquilo exposto aqui e mesmo nas discussões do sistema por nós proposto esse será um tema que permanecerá em segundo plano, uma vez que diz respeito a uma extensa área de estudo. Entretanto, muito do que foi discutido aqui será subentendido quando exposto e analisarmos nosso sistema.

Torna-se difícil seguir uma seqüência histórica bastante aprofundada, uma vez que o ponto mais interessante seria o desenvolvimento de sistemas criptográficos no domínio totalmente óptico. Dispositivos como o que iremos propor não são encontrados com facilidade na literatura, motivo pelo qual pouca referência será apresentada. Tal ausência também prejudica a comparação da eficiência de nosso dispositivo. Não há interesse em

compará-lo com sistemas híbridos, uma vez que o interesse moderno, como já discutido, está em desenvolver equipamentos que funcionem apenas no domínio óptico.

1.6 Referências Bibliográficas

[1] ACKERMANN, Marsha E. et al. Encyclopedia of World History. Facts On File Library Of World History, 2008. IV.

[2] RAY, John. The Rosetta Stone and the Rebirth of Ancient Egypt. Profile Books Ltd, 2008.

[3] POPE, Maurice. The Story of Archaeological Decipherment: From Egyptian Hieroglyphs to Linear B. Scribner, 1975.

[4] YOUNG, Thomas. Rudiments of an Egyptian dictionary in the ancient enchorial character. John & Arthur Arch, 1831.

[5] HONOUR, Alan. The man who could read stones: Champollion and the Rosetta Stone. Hawthorn Books, 1966.

[6] ADKINS, Lesley; ADKINS, Roy A.. The keys of Egypt: the race to read the hieroglyphs. Harper Collins, 2001.

[7] EDWARD, Bleiberg (Ed.). Arts and Humanities Through the Eras: Ancient Egypt - 2675-332 B.C.. Thomson Gale, 2005.

[8] TYLDESLEY, Joyce A.. Egypt: how a lost civilization was rediscovered. California: University Of California Press, 2006.

[9] HAWKINS, Gerald S.. Beyond Stonehenge. Harper & Row, 1973.

[10] CHURCHHOUSE, R. F.. Codes and ciphers: Julius Caesar, the Enigma and the internet. Cambridge: Cambrige University Press, 2004.

[11] MOLLIN, Richard A.. Codes: The Guide to Secrecy from Ancient to Modern Times. Chapman & Hall/crc, 2005.

[12] MOLLIN, Richard A.. An Introduction to Cryptography. 2. ed. Chapman & Hall/crc, 2007.

[13] LUBBE, Jan C.a. Van Deer. Basic Methods of Criptography. Cambridge: Cambridge University Press, 1999.

[14] OPPLIGER, Rolf. Contemporary Cryptography. Artch House Inc., 2005.

[15] KONHEIM, Alan G.. Computer Security and Cryptography. New Jersey: John Wiley & Sons, 2007.

[16] BUCHMANN, Johannes A.. Introdução à Criptografia. São Paulo: Berkeley, 2002.

[17] SCHNEIER, Ferguson B.. Practical Cryptography. New York: John Wiley & Sons, 2003.

[18] BOYD, C.; MATHURIA, A.. Protocols for Key Establishment and Authentication. New York: Springer-verlag, 2003.

[19] SMITH, R. E.. Authentication: From Passwords to Public Keys. Massachusetts: Addison-Wesley, 2001.

[20] DELFS, H.; KNEBL, H.. Introduction to Cryptography: Principles and Applications. 2. ed. Springer, 2007.
[21] MOLDOVYAN, Nick; MOLDOVYAN, Alex. Innovative Cryptography. 2. ed. Boston, Massachusetts: Charles River Media, 2007.

[22] COPPERSMITH, D.. The Data Encryption Standard (DES) and Its Strength Against Attacks. IBM Journal Of Research And Development, p. 243-250. 1994.

[23] BIHAM, E.; SHAMIR, A.. Differential Cryptanalysis of DES. Springer-Verlag, 1993.

[24] HIGGINS, Peter M.. Number Story: From Counting to Cryptography. Copernicus Books, 2000.

[25] MOLLIN, Richard A. et al. An introduction to cryptography, Discrete mathematics and its applications. 2. ed. CRC Press, 2007.

[26] KONHEIM, G. A. et al. Computer Security and Cryptography, Discrete mathematics and its applications. John Wiley & Sons, Inc., Publication, 2007.

[27] BELLARE, M. et al. Trapdoor Functions and Public-Key CryptosystemsTrapdoor Functions. In: CRYPTO98, 23., Springer-Verlag Lecture Notes in Computer Science. 1998. v. 1462, p. 283 - 298.

[28] WELSH, Dominic. Codes and Cryptography. Oxford: Oxford University Press, 1988.

[29] BIGGS, Norman L.. Codes: An Introduction to Information Communication and Cryptography: Springer, 2008. (Springer Undergraduate Mathematics Series).

[30] KOBLITZ, N.. A Course in Number Theory and Cryptography. New York: Springer-Verlag, 1994.

[31] SEBASTOPOL. Cracking DES: Secrets of Encryption Research, WiretapPolitics & Chip Design. Electronic Frontier Foundation (EFF), Califórnia, 1998.

[32] DIFFIE, W; HELLMAN, M.. New Directions in Cryptography. IEEE Transactions On Information Theory, p.644-654, 1976.

[33] MERKLE, R. C.; HELLMAN, M.e.. Secure Communication over an Insecure Channel. Commun. Ass. Comp. Mach, Pppp, v. 21, n. , p.294-299, 1978.

2 EFEITO ACÚSTICO-ÓPTICO

O efeito acústico-óptico, teoricamente previsto em 1922 [1] e somente realizado experimentalmente dez anos depois [2], trata com a interação de ondas ópticas com ondas acústicas em um meio material. A diferença na ordem de grandeza entre esses dois tipos de onda torna impossível qualquer interação direta entre elas. Dessa forma, essa interação se dá de forma indireta, através do uso de um meio material para tal.

Consideremos uma onda plana de luz monocromática em um meio excitado por uma onda acústica modulando periodicamente o índice de refração de tal meio. Este se torna então periódico cujo período é igual ao do comprimento de onda da onda acústica. Tal perturbação periódica é função tanto do espaço quanto do tempo. A perturbação periódica se move na velocidade da onda sonora (algo em torno de 10^3 m/s). Uma vez que a velocidade do som é algo em torno de cinco ordens de grandezas menor que a da luz, a perturbação periódica causada pela onda de som pode ser considerada estacionária. O problema se reduz, portanto, ao da propagação eletromagnética em um meio periódico.

Quando uma onda acústica se propaga num meio, existe um campo de tensão associado a esta onda. Tal tensão surge da mudança no índice de refração. Isto é chamado de efeito foto-elástico. A interação acústico-óptica oferece uma forma conveniente de manipular uma radiação ***laser***. A modulação da luz pela interação acústico-óptica é utilizada em um grande número de aplicações [3]. Entretanto, nos dedicaremos, por uma questão de relação com os objetivos principais do presente trabalho, apenas aos filtros sintonizáveis.

De posse de um conjunto de equações acopladas obtidas a partir das Equações de Maxwell, consideraremos uma variação periódica no tensor dielétrico do meio, ao longo da direção *z*. Isso determinará a amplitude de cada modo ao longo do comprimento do dispositivo. A descrição matemática da propagação de cada modo no dispositivo permitirá obter e comparar as soluções analítica e numérica das características de transmissão de um AOTF, utilizando-se de métodos numéricos tradicionais. Tais características resumem-se na eficiência de conversão de energia entre os modos e na curva de transmissão do dispositivo.

2.1 Teoria Eletromagnética

2.1.1 Polarização de Ondas de Luz

Muitos casos envolvendo a propagação de ondas de luz dependem crucialmente da direção de oscilação do campo elétrico, assim o vetor campo elétrico **E** é escolhido para definir o estado de polarização das ondas de luz. Tal escolha é conveniente porque, na maioria dos meios ópticos, interações físicas com a onda envolvem o campo elétrico. A principal razão para se estudar a polarização da luz é que em muitas substâncias (meios anisotrópicos) o índice de refração depende da direção de oscilação do vetor campo elétrico **E**. Este fenômeno pode ser explicado em termos do movimento dos elétrons que são direcionados pelo campo elétrico das ondas de luz [3].

A polarização da luz é especificada pelo vetor campo elétrico **E**(**r**,t) em um ponto fixo do espaço, **r**, em um tempo t. Para uma onda monocromática, a variação temporal do campo elétrico é sinusoidal, ou seja, o campo elétrico deve oscilar em uma freqüência definida. Se assumirmos que a luz esteja se propagando na direção de z, o campo elétrico se manterá no plano xy. Uma vez que as componentes x e y podem oscilar independentemente em uma freqüência definida, deve-se considerar o efeito produzido pela adição vetorial dessas duas componentes oscilando ortogonalmente.

O problema de superpor duas oscilações independentes em ângulos retos e com a mesma freqüência é bem conhecido e análogo ao clássico movimento de um oscilador harmônico bidimensional. O movimento geral do oscilador é uma elipse, que corresponde à oscilação na qual x e y não estão em fase [3]. Numa representação na forma complexa, o vetor campo elétrico propagando-se na direção z pode ser escrito como:

$$\vec{E}(z,t) = \mathrm{Re}\left[\vec{A}\, e^{i(\omega t - kz)}\right] \qquad (2.1.1)$$

onde **A** é um vetor complexo que permanece no plano *xy*. Consideraremos agora a natureza da curva cujo ponto final do vetor campo elétrico **E** descrito em um ponto típico no espaço. Esta curva é o ***locus*** da evolução temporal dos pontos cujas coordenadas (E_x, E_y) são:

$$E_x = A_x \cos(\omega t - kz + \delta_x) \tag{2.1.2}$$

$$E_y = A_y \cos(\omega t - kz + \delta_y) \tag{2.1.3}$$

onde o vetor complexo **A** foi definido como $\vec{A} = \hat{x} A_x e^{i\delta x} + \hat{y} A_y e^{i\delta y}$,onde A_x e A_y são números positivos e $\hat{x}$ e $\hat{y}$ são vetores unitários. A curva descrita pelo ponto final do vetor elétrico, quando o tempo evolui, pode ser obtida pela eliminação de $(\omega t - kz)$ entre as equações (2.1.2) e (2.1.3), resultando em [4]:

$$\left(\frac{E_x}{A_x}\right)^2 + \left(\frac{E_y}{A_y}\right)^2 - \frac{2\cos\delta}{A_x A_y} E_x E_y = sen^2\delta \ , \tag{2.1.4}$$

onde $\delta = \delta_y - \delta_x$. Todos os ângulos de fase são definidos na razão $-\pi < \delta \leq \pi$.

A equação (2.1.4) é a equação de uma cônica. De (2.1.2) e (2.1.3) é possível ver que a cônica está confinada em uma região regular cujos lados são paralelos aos eixos coordenados e cujos comprimentos são $2A_x$ e $2A_y$. Portanto, a curva deve ser uma elipse. A onda (2.1.1) é dita elipticamente polarizada. Uma descrição completa da polarização elíptica inclui a orientação da elipse com respeito aos eixos coordenados e o sentido de revolução de **E**. Em geral, os eixos principais da elipse não estão nas direções ***x*** e ***y***. Entretanto, através de uma rotação do sistema de coordenadas, podemos diagonalizar a equação (2.1.4). Seja *x*' e *y*' o novo grupo de eixos principais da elipse, então a equação da elipse no novo sistema de coordenadas torna-se:

$$\left(\frac{E'_x}{a}\right)^2 + \left(\frac{E'_y}{b}\right)^2 = 1 \ , \tag{2.1.5}$$

onde *a* e *b* são os eixos principais da elipse e E'_x e E'_y as componentes do vetor campo elétrico neste sistema de coordenadas. Seja ϕ ($0 \leq \phi < \pi$) o ângulo entre a direção do eixo maior *x*' e o eixo *x*, então os comprimentos dos eixos principais são dados por:

$$a^2 = A_x^2 \cos^2\phi + A_y^2 sen^2\phi + 2A_xA_y \cos\delta \cos\phi sen\phi \,, \tag{2.1.6}$$

$$b^2 = A_x^2 sen^2\phi + A_y^2 \cos^2\phi - 2A_xA_y \cos\delta \cos\phi sen\phi \,. \tag{2.1.7}$$

O ângulo ϕ pode ser expresso em termos de A_x, A_y e $\cos\delta$ como:

$$tg\,2\phi = \frac{2A_xA_y}{A_x^2 - A_y^2}\cos\delta \,. \tag{2.1.8}$$

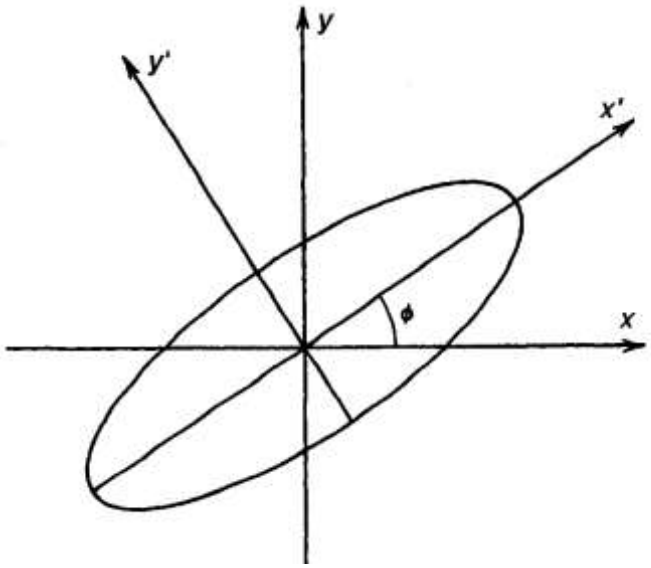


FIGURA 2.1: Polarização elíptica típica.

O sentido da revolução de uma polarização elíptica é determinado pelo sinal de senδ. O ponto final do vetor elétrico se movimentará no sentido dos ponteiros do relógio se senδ >0 e no sentido contrário se senδ<0. As mudanças na polarização elíptica com relação à variação da diferença do fator δ podem ser encontradas facilmente na literatura [4].

2.1.2 Propagação Eletromagnética em Meios Anisotrópicos

Há muitos materiais cujas propriedades ópticas dependem tanto da direção de propagação quanto da polarização da luz. Tais materiais opticamente anisotrópicos incluem cristais como calcita, quartzo e KDP, assim como cristais líquidos [4]. Eles exibem muitos fenômenos ópticos interessantes como efeitos de polarização, eletro-ópticos e acústico-ópticos. Um completo entendimento da propagação da luz em meio anisotrópico passa a ser importante quando esses fenômenos são usados em aplicações práticas.

Em um meio isotrópico a polarização induzida é sempre paralela ao campo elétrico e está relacionada a ele por um fator escalar (a susceptibilidade) que é independente da direção ao longo do qual o campo é aplicado. Isto não é sempre verdade em meio anisotrópico, exceto para certas direções particulares. Uma vez que o cristal é feito de uma cadeia regular de átomos (ou moléculas) com certa simetria, nós devemos esperar que a polarização induzida fosse depender, ambos em sua magnitude e direção, sobre a direção do campo aplicado. Em vez de uma função escalar simples ligando **P** e **E**, temos:

$$P_x = \varepsilon_0(\chi_{11}E_x + \chi_{12}E_y + \chi_{13}E_z), \tag{2.1.9}$$

$$P_y = \varepsilon_0(\chi_{21}E_x + \chi_{22}E_y + \chi_{23}E_z), \tag{2.1.10}$$

$$P_z = \varepsilon_0(\chi_{31}E_x + \chi_{32}E_y + \chi_{33}E_z), \tag{2.1.11}$$

onde as letras maiúsculas denotam as amplitudes complexas. A matriz 3×3 dos coeficientes χ_{ij} é chamada tensor de susceptibilidade elétrica e a magnitude dos χ_{ij} depende da escolha dos eixos *x*, *y* e *z* da estrutura do cristal[15]. Podemos ainda descrever a resposta dielétrica do cristal por meio do tensor de permissividade dielétrica ε_{ij}, definido por

$$D_i = \varepsilon_{ij}E_j \tag{2.1.12}$$

onde a convenção sobre índices repetidos é observada. Considerações sobre a conservação da energia do campo eletromagnético requerem que o tensor dielétrico seja Hermitiano [4],

[15] É sempre possível escolher tais eixos de tal forma que os elementos fora da diagonal desapareçam, deixando $P_x = \varepsilon_0\chi_{11}E_x$, $P_y = \varepsilon_0\chi_{22}E_y$, $P_z = \varepsilon_0\chi_{33}E_z$. Estas direções são chamadas de ***eixos dielétricos principais*** do cristal.

$\varepsilon_{ij} = \varepsilon^{*}_{ji}$; o que, no caso especial em que o tensor dielétrico torna-se real, a propriedade Hermitiana reduz-se às propriedades de simetria. Das equações (2.1.9) – (2.1.11) e da relação $\vec{D} = \varepsilon_0 \vec{E} + \vec{P}$, temos que $\varepsilon_{ij} = \varepsilon_0 (1 + \chi_{ij})$. Estas nove quantidades são constantes do meio e constituem o tensor dielétrico.

A densidade de energia armazenada num campo elétrico em um meio anisotrópico é dada por:

$$U_e = \frac{1}{2} \vec{E} \cdot \vec{D} = \frac{1}{2} E_i \varepsilon_{ij} E_j . \qquad (2.1.13)$$

É possível associar a essa densidade de energia uma superfície com U_e constante, no espaço $\vec{D}$, podendo ser escrita como [4]:

$$\frac{D_x^2}{\varepsilon_x} + \frac{D_y^2}{\varepsilon_y} + \frac{D_z^2}{\varepsilon_z} = 2U_e \qquad (2.1.14)$$

onde ε_x, ε_y e ε_z são os valores das constantes dielétricas nos eixos principais. Se trocarmos $\vec{D} / \sqrt{2U_e}$ por $\vec{r}$ e definirmos os principais índices de refração n_x, n_y e n_z por $n_i^2 \equiv \varepsilon_i / \varepsilon_0$ ($i = x, y$ e z), a última equação pode ser escrita como

$$\frac{x^2}{n_x^2} + \frac{y^2}{n_y^2} + \frac{z^2}{n_z^2} = 1 . \qquad (2.1.15)$$

Esta equação é a equação geral do elipsóide com os eixos maiores paralelos aos eixos x, y e z, cujos comprimentos respectivos são $2n_x$, $2n_y$ e $2n_z$. O elipsóide é conhecido como ***índice elipsóide*** e é usado principalmente para encontrar os dois índices de refração e as duas direções correspondentes de $\vec{D}$ associadas com as duas ondas planas independentes que podem propagar ao longo de uma direção arbitrária $\vec{s}$ em um cristal. Faz-se isto da seguinte forma: encontra-se as interseções da elipse entre um plano através da origem que é normal a direção de propagação $\vec{s}$ e o índice elipsóide. Os dois eixos de intersecção da elipse são iguais em comprimento a $2n_1$ e $2n_2$, onde n_1 e n_2 são os índices de refração. Estes dois eixos são paralelos, respectivamente, às direções dos vetores $\vec{D}_{1,2}$ das duas soluções permitidas (veja FIGURA 2.2).

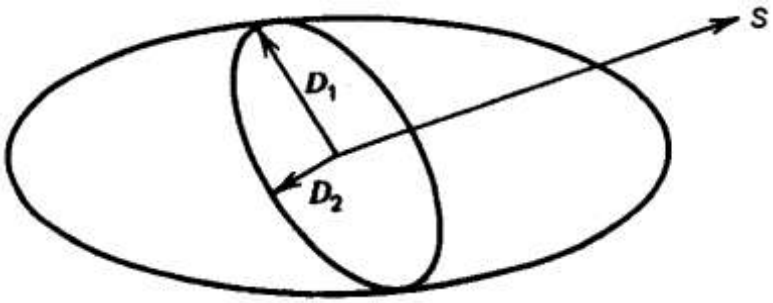


FIGURA 2.2: Método do índice elipsóide. A elipse interna é a intersecção do índice elipsóide com o plano normal a **S**.

A superfície normal é unicamente determinada pelos índices n_x, n_y e n_z. No caso geral, quando os três índices são diferentes, há dois eixos ópticos. O cristal é dito então biaxial. Em muitos materiais, acontece de dois dos índices serem iguais, onde $n_o^2 = \varepsilon_x/\varepsilon_o = \varepsilon_y/\varepsilon_o$ e $n_e^2 = \varepsilon_z/\varepsilon_o$. Aqui, n_o é chamado índice ordinário e n_e, índice extraordinário. Se $n_o<n_e$, o cristal é dito positivo; se $n_o>n_e$, o cristal é dito negativo. A superfície normal neste caso consiste de uma esfera e um elipsóide de revolução. As duas folhas da superfície normal se tocam em dois pontos do eixo *z*. O eixo *z* é portanto o único eixo óptico e o cristal é dito ser uniaxial. Se todos os três eixos são iguais, as duas folhas da superfície normal degeneram em uma esfera e o cristal é opticamente isotrópico.

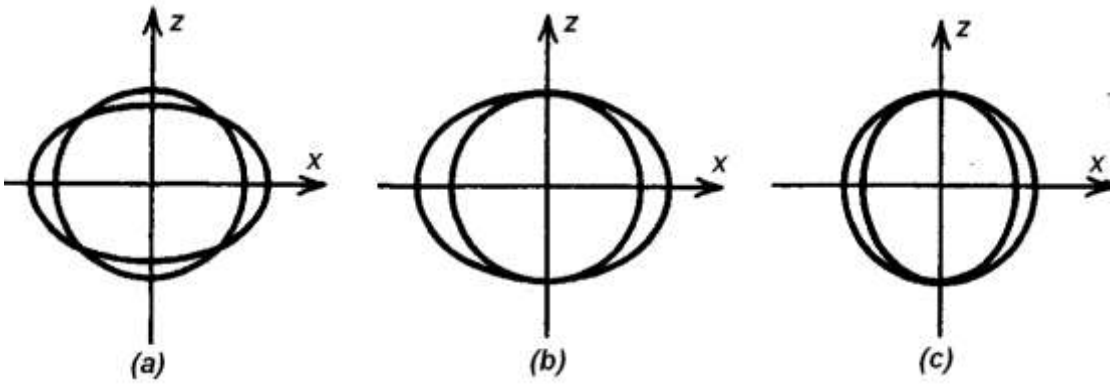


FIGURA 2.3: Intersecção da superfície normal para com o plano *xy* para (a) cristais biaxiais, (b) cristais uniaxiais positivos, (c) cristais uniaxiais negativos.

É óbvio que simetria óptica de um cristal está relacionada ao grupo de ponto do cristal. Por exemplo, num cristal cúbico, os três eixos principais são fisicamente equivalentes. Portanto, espera-se que um cristal cúbico seja isotrópico. É possível encontrar tabelas que

relacionam a simetria óptica dos cristais com o tensor dielétrico[16]. Muitos dispositivos ópticos envolvem o uso de cristais uniaxiais. Nestes cristais, o índice elipsóide resume-se a:

$$\frac{x^2}{n_o^2} + \frac{y^2}{n_o^2} + \frac{z^2}{n_e^2} = 1 \,. \tag{2.1.16}$$

onde o eixo de simetria tem sido escolhido como o eixo *z* [4].

2.2 Propagação Eletromagnética em Meios Periódicos e Teoria dos Modos Acoplados

2.2.1 Propagação Eletromagnética em Meios Periódicos

A propagação da radiação eletromagnética em meios periódicos é de suma importância para o entendimento do funcionamento do AOTF. As propriedades ópticas de um meio periódico são descritas pelos tensores dielétricos e de permissividade, que, refletindo a simetria translacional do meio, são funções periódicas de **x**:

$$\varepsilon(\mathbf{x}) = \varepsilon(\mathbf{x}+\mathbf{a}), \tag{2.2.1}$$

$$\mu(\mathbf{x}) = \mu(\mathbf{x}+\mathbf{a}), \tag{2.2.2}$$

onde **a** é qualquer vetor arbitrário da rede. A propagação de uma radiação monocromática (***laser***), de freqüência ω, em um meio periódico é descrito pelas equações de Maxwell,

$$\nabla \times \vec{H} = i\omega\varepsilon \vec{E} \,, \tag{2.2.3}$$

$$\nabla \times \vec{E} = -i\omega\mu \vec{H} \,. \tag{2.2.4}$$

[16] O $LiNbO_3$, cristal utilizado nas simulações que realizamos, é um cristal uniaxial negativo com n_o=2.300 e n_e=2.208.

Estas equações não se alteram deslocadas de **a**. Uma solução exata destas duas equações é possível apenas em alguns casos como, por exemplo, em meios periódicos unidimensionais mais comuns, os quais são construídos com camadas alternantes de índice de refração diferentes, tendo uma determinada periodicidade rigorosamente controlada [6-9]. Existem muitos outros meios periódicos em que apenas uma solução aproximada das equações de Maxwell pode ser obtida. Um dos métodos de resolução é conhecido como teoria dos modos acoplados. Nela, uma variação periódica no tensor dielétrico é considerada como uma perturbação que acopla os modos normais não perturbados, provocando um intercâmbio de energia entre os respectivos modos acoplados. Em outras palavras, o tensor dielétrico, apresentado nas equações de Maxwell, terá uma dependência espacial com um novo aspecto dado por:

$$\varepsilon(x, y, z) = \varepsilon_o(x, y) + \Delta\varepsilon(x, y, z), \tag{2.2.5}$$

onde $\varepsilon_o(x,y)$ é a parte não perturbada do tensor dielétrico e $\Delta\varepsilon(x,y,z)$ representa a parte do tensor dielétrico que varia periodicamente. Assumimos que os modos normais de propagação no meio dielétrico não perturbado descrito pelo tensor dielétrico $\varepsilon_o(x,y)$ são conhecidos.

Uma vez que o meio dielétrico não perturbado é homogêneo na direção z, os modos normais podem ser escritos na forma:

$$E_m(x, y)\exp[\ i(\omega t - \beta_m z)], \tag{2.2.6}$$

onde o índice *m* pode ser contínuo para modos desacoplados, como ondas planas, ou discretos para modos confinados, tais como modos de guias de onda. Se um campo arbitrário, com freqüência ω, é excitado em z=0, a propagação deste campo no meio não perturbado pode sempre ser expresso em termos de uma combinação linear dos modos normais:

$$\vec{E} = \sum_m A_m \vec{E}_m(x, y)\exp[\ i(\omega t - \beta_m z)], \tag{2.2.7}$$

onde os termos A_m são constantes. Tal expansão é possível porque esses modos normais formam um conjunto completo [10]. Tais modos são geralmente normalizados a uma potência

de 1W na direção z. Desse modo, a relação de ortogonalidade dos modos pode ser escrita como:

$$\frac{1}{2}\int (\vec{E}_l \times \vec{H}^*_k)_z \, dxdy = \delta_{lk} \ , \tag{2.2.8}$$

onde $\mathbf{H}_k$ é o campo magnético associado ao modo $\mathbf{E}_k$.

Consideraremos a seguir a propagação de um modo não perturbado $\mathbf{E_1}(x,y)\exp[i(\omega t-\beta_1 z)]$ em um meio perturbado descrito pelo tensor dielétrico $\varepsilon_o(x,y) + \Delta\varepsilon(x,y,z)$. A presença da perturbação dielétrica $\Delta\varepsilon(x,y,z)$ causa o surgimento de uma nova perturbação na polarização

$$\Delta\vec{P} = \Delta\varepsilon(x,y,z)\vec{E}_1(x,y)\exp[\ i(\omega t - \beta_1 z)] \ . \tag{2.2.9}$$

Se esta onda de polarização pode alimentar a energia do outro modo $\mathbf{E_2}(x,y)\exp[i(\omega t-\beta_2 z)]$. Dizemos então que o perturbação dielétrica $\Delta\varepsilon(x,y,z)$ acopla (ou seja, causa a troca de energia) entre os modos $\mathbf{E_1}$ e $\mathbf{E_2}$ [11].

Escreveremos agora o vetor campo elétrico da onda eletromagnética como uma expansão nos modos normais da estrutura dielétrica não perturbada, onde os coeficientes de expansão evidentemente dependem de z, uma vez que $\Delta\varepsilon \neq 0$ as ondas $E_m(x,y)\exp[i(\omega t-\beta_m z)]$ não são sempre automodos:

$$\vec{E} = \sum_m A_m(z)\vec{E}_m(x,y)\exp[\ i(\omega t - \beta_m z)] \ . \tag{2.2.10}$$

Substituindo tal equação na equação de onda, temos [11]:

$$\{\nabla^2 + \omega^2\mu[\varepsilon_o(x,y) + \Delta\varepsilon(x,y,z)]\}\vec{E} = 0 \tag{2.2.11}$$

e sabendo que os modos normais satisfazem:

$$\left[\frac{\partial^2}{\partial x^2}+\frac{\partial^2}{\partial y^2}+\omega^2\mu\varepsilon_o(x,y)-\beta_m^2\right]\vec{E}_m(x,y)=0\ . \qquad (2.2.12)$$

Temos, então:

$$\sum_m\left[\frac{d^2}{dz^2}A_k-2i\beta_k\frac{d}{dz}A_k\right]\vec{E}_k(x,y)\exp(-i\beta_k z)=-\omega^2\mu\sum_l\Delta\varepsilon(x,y,z)A_l\vec{E}_l(x,y)\exp(-i\beta_l z)\ . \qquad (2.2.13)$$

Assumimos, além disso, que a perturbação é “fraca”, de tal forma que a variação da amplitude é “lenta” e satisfaz a condição [5]:

$$\left|\frac{d^2}{dz^2}A_k\right|<<\left|\beta_k\frac{d}{dz}A_k\right|. \qquad (2.2.14)$$

Esta condição é conhecida como aproximação parabólica e é freqüentemente usada em pequenas perturbações. Destarte, negligenciando as segundas derivadas em (2.2.14), temos:

$$-2i\sum_k\beta_k\left(\frac{d}{dz}A_k\right)\vec{E}_k(x,y)\exp(-i\beta_k z)=-\omega^2\mu\sum_l\Delta\varepsilon(x,y,z)A_l\vec{E}_l(x,y)\exp(-i\beta_k z)\ . \qquad (2.2.15)$$

Tomamos então o produto escalar de (2.2.15) com $\vec{E}_k^{\,*}(x,y)$ e integramos sobre *x* e *y*. Usando então as propriedades de ortogonalidade:

$$\langle k\mid k\rangle\frac{d}{dz}A_k(z)=\frac{\omega^2\mu}{2i\beta_k}\sum_l\langle k\mid\Delta\varepsilon\mid l\rangle A_l(z)\exp[i(\beta_k-\beta_l)z]\ , \qquad (2.2.16)$$

onde

$$\langle k\mid k\rangle\equiv\int\vec{E}_k^{\,*}(x,y)\cdot\vec{E}_k(x,y)\,dxdy=\frac{2\omega\mu}{|\beta_k|}, \qquad (2.2.17)$$

$$\left\langle k \mid \Delta\varepsilon \mid l \right\rangle \equiv \int \vec{E}_k^{\,*}(x,y)\cdot\Delta\varepsilon(x,y,z)\,\vec{E}_k^{\,*}(x,y)\,dxdy \quad . \tag{2.2.18}$$

Uma vez que a perturbação $\Delta\varepsilon(x, y, z)$ é periódica em z, é possível expandi-la como uma série de Fourier:

$$\Delta\varepsilon(x,y,z) = \sum_{m\neq 0} \varepsilon_m(x,y)\exp\left(-im\,\frac{2\pi}{\Lambda}z\right), \tag{2.2.19}$$

onde a soma se dá sobre todos os m com exceção de m=0 devido a definição de $\Delta\varepsilon(x, y, z)$ em (2.2.5). Substituindo as equações (2.2.19), (2.2.18) e (2.2.17) em (2.2.15), temos:

$$\frac{d}{dz}A_k(z) = -i\,\frac{\beta_k}{|\beta_k|}\sum_l\sum_m C_{kl}^{(m)}A_l\exp[\;i(\beta_k-\beta_l-m\,2\pi/\Lambda)z\,], \tag{2.2.20}$$

onde o coeficiente (constante) de acoplamento $C_{kl}^{(m)}$ é definido como

$$C_{kl}^{(m)} \equiv \frac{\omega}{4}\left\langle k \mid \varepsilon_m \mid l \right\rangle = \frac{\omega}{4}\int \vec{E}_k^{\,*}(x,y)\cdot\varepsilon_m(x,y)\,\vec{E}_l^{\,*}(x,y)\,dxdy \quad . \tag{2.2.21}$$

O coeficiente $C_{kl}^{(m)}$ reflete a magnitude do acoplamento entre o k-ésimo modo e o l-ésimo devido ao m-ésimo componente de Fourier da perturbação dielétrica.

2.2.2 Equações do Modo Acoplado

A equação (2.2.20) constitui um conjunto de equações diferenciais lineares acopladas. Em princípio, um número infinito de modos de amplitudes está envolvido. Na prática, especialmente próxima à região de acoplamento ressonante[17], apenas dois modos são

[17] O acoplamento ressonante ocorre quando

$$\beta_k - \beta_l - m\,\frac{2\pi}{\Lambda} = 0$$

para algum inteiro m. Esta condição é de fundamental importância e nós nos referiremos à ela como "descasamento de fase longitudinal" ou apenas ***descasamento de fase***. Esta condição é o análogo espacial da conservação da energia na teoria da perturbação com dependência temporal e deve ser chamada de conservação do momento. Uma visão mais completa pode ser encontrada em [4].

fortemente acoplados, e a equação reduz-se apenas a duas equações para estes dois modos. Designaremos estes dois modos por 1 e 2. Desconsiderando a interação com quaisquer outros modos, as equações de modos acoplados tornam-se

$$\frac{d}{dz} A_1 = -i \frac{\beta_1}{|\beta_1|} C_{12}^{(m)} A_2 \exp(-i\Delta\beta_z) \tag{2.2.22}$$

$$\frac{d}{dz} A_2 = -i \frac{\beta_2}{|\beta_2|} C_{21}^{(-m)} A_1 \exp(-i\Delta\beta_z) \tag{2.2.23}$$

onde

$$\Delta\beta = \beta_1 - \beta_2 - m\frac{2\pi}{\Lambda} \tag{2.2.24}$$

e $C_{12}^{(m)}, C_{21}^{(-m)}$ são as constantes de acoplamento dadas pela equação (2.2.21). Quando o tensor dielétrico é função apenas de *z*, os modos normais do meio não-perturbado são ondas planas e os coeficientes de Fourier ε_m da perturbação dielétrica são constantes. As constantes de acoplamento para esse caso especial tornam-se:

$$C_{kl}^{(m)} = \frac{\omega^2 \mu}{2\sqrt{|\beta_k \beta_l|}} \vec{p}_k \cdot \varepsilon_m \vec{p}_l, \tag{2.2.25}$$

onde $\vec{p}_k$ e $\vec{p}_l$ são os vetores unitários de polarização das ondas planas. As constantes de acoplamento (2.5.4) dependem tanto do estado de polarização dos modos acoplados quanto do próprio tensor da expansão dos coeficientes de Fourier para ε_m. O sinal dos fatores $\beta_1/|\beta_1|$ e $\beta_2/|\beta_2|$ nas equações do modo acoplado são de suma importância e irão determinar o comportamento do acoplamento. Tais sinais dependem da direção de propagação dos modos acoplados. Destarte, podemos dividir o acoplamento em dois tipos: acoplamento codirecional e contradirecional[18].

2.2.3 Acoplamento Codirecional

[18] Geralmente os filtros acústico-ópticos empregam a interação codirecional com grandes ângulos. Dessa forma, não nos debruçaremos sobre o problema contradirecional. Entretanto, ao leitor interessado, indicamos a referência [4].

Quando os modos acoplados estão propagando na mesma direção, *z*, por exemplo, os sinais dos fatores $\beta_1/|\beta_1|$ e $\beta_2/|\beta_2|$ são ambos positivos. As equações do modo acoplado tornam-se:

$$\frac{d}{dz} A_1 = -i\kappa A_2 \exp(-i\Delta\beta_z) , \tag{2.2.26}$$

$$\frac{d}{dz} A_2 = -i\kappa^* A_1 \exp(-i\Delta\beta_z) , \tag{2.2.27}$$

onde

$$\kappa = C_{12}^{(m)} . \tag{2.2.28}$$

Deve-se lembrar que A_1 e A_2 são amplitudes complexas dos modos normalizados. Assim, $|A_1|$ e $|A_2|$ representam os fluxos de potência nos modos 1 e 2 respectivamente. As equações dos modos acoplados são consistentes com a conservação da energia que requer que

$$\frac{d}{dz}\{|A_1|^2 + |A_2|^2\} = 0 . \tag{2.2.29}$$

As soluções gerais das equações (2.2.26) e (2.2.27) são:

$$A_1(z) = \exp[-i(\Delta\beta/2)z]\left\{\left[\cos(sz) - i\frac{\Delta\beta}{2s}sen(sz)\right]A_1(0) - i\frac{\kappa}{s}sen(sz)A_2(0)\right\} , \tag{2.2.30}$$

$$A_2(z) = \exp[-i(\Delta\beta/2)z]\left\{-i\frac{\kappa^*}{s}sen(sz)A_1(0) + \left[\cos(sz) + i\frac{\Delta\beta}{2s}sen(sz)\right]A_2(0)\right\} , \tag{2.2.31}$$

onde

$$s^2 = \kappa^*\kappa + \left(\frac{\Delta\beta}{2}\right)^2 , \tag{2.2.32}$$

e $A_1(0)$ e $A_2(0)$ são as amplitudes em z = 0. De (2.2.30) e (2.2.31) é possível observar que fração de potência que é acoplada do modo A_2 para o modo A_1, em uma distância z, ou vice-versa, é:

$$\frac{|\kappa|^2}{|\kappa|^2 + (\Delta\beta/2)^2} \operatorname{sen}^2\sqrt{|\kappa|^2 + \left(\frac{\Delta\beta}{2}\right)^2}\, z\,. \qquad (2.2.33)$$

A fração máxima de potência trocada é $|\kappa|^2/[|\kappa|^2+(\Delta\beta/2)^2]$, possuindo seu menor valor quando $\Delta\beta>>|\kappa|$. A completa transferência de energia ocorre quando $\Delta\beta=0$, ou seja, quando o encontro de fase é obtido.

2.3 Efeito Fotoelástico.

O efeito fotoelástico em um material acopla uma perturbação (tensão) mecânica ao índice de refração óptico. Este efeito ocorre em todos os estados da matéria e é tradicionalmente descrito por:

$$\Delta\eta_{ij} = \Delta\left(\frac{1}{n^2}\right)_{ij} = p_{ijkl}\, S_{kl}\,, \qquad (2.3.1)$$

onde $\Delta\eta_{ij}$ [ou $\Delta(1/n^2)_{ij}$] é a mudança no tensor de impermeabilidade óptica e S_{kl} é o tensor da perturbação mecânica. Os coeficiente p_{ijkl} formam o tensor óptico-mecânico. Na equação (2.3.1), termos de alta ordem envolvendo as potências de S_{kl} são negligenciados porque estes termos são muito pequenos se comparados com o termo linear (S_{kl} é tipicamente da ordem de 10^{-5}). O índice elipsóide de um cristal na presença de uma perturbação mecânica aplicada é dado por:

$$\left(\eta_{ij} + p_{ijkl}\, Skl\right) x_i x_j = 1\,. \qquad (2.3.2)$$

Quando S_{kl}=0, o índice elipsóide reduz-se a:

$$\frac{x^2}{n_x^2} + \frac{y^2}{n_y^2} + \frac{z^2}{n_z^2} = 1 \qquad (2.3.3)$$

no sistema principal de coordenadas. Uma vez que ambos η_{ij} e S_{kl} são tensores simétricos, os índices *i* e *j*, assim como o *k* e o *l*, podem ser permutados. Assim, torna-se conveniente usar índices contraídos na notação. A equação (2.3.1) pode então ser escrita como:

$$\Delta\left(\frac{1}{n^2}\right)_i = p_{ij} S_j, \qquad i, j = 1,2, ..., 6, \tag{2.3.4}$$

onde S_j são as componentes da tensão mecânica. A equação do índice elipsóide pode agora ser escrita como:

$$\begin{aligned}
&x^2\left(\frac{1}{n_x^2} + p_{11}S_1 + p_{12}S_2 + p_{13}S_3 + p_{14}S_4 + p_{15}S_5 + p_{16}S_6\right)\\
&+ y^2\left(\frac{1}{n_y^2} + p_{21}S_1 + p_{22}S_2 + p_{23}S_3 + p_{24}S_4 + p_{25}S_5 + p_{26}S_6\right)\\
&+ z^2\left(\frac{1}{n_z^2} + p_{31}S_1 + p_{32}S_2 + p_{33}S_3 + p_{34}S_4 + p_{35}S_5 + p_{36}S_6\right)\\
&+ 2yz\left(p_{41}S_1 + p_{42}S_2 + p_{43}S_3 + p_{44}S_4 + p_{45}S_5 + p_{46}S_6\right)\\
&+ 2zx\left(p_{51}S_1 + p_{52}S_2 + p_{53}S_3 + p_{54}S_4 + p_{55}S_5 + p_{56}S_6\right)\\
&+ 2xy\left(p_{61}S_1 + p_{62}S_2 + p_{63}S_3 + p_{64}S_4 + p_{65}S_5 + p_{66}S_6\right) = 1
\end{aligned} \tag{2.3.5}$$

onde n_x, n_y e n_z são os índices de refração no sistema de coordenadas principal. Os coeficientes p_{ij} são geralmente definidos no sistema de coordenadas principal. O novo índice elipsóide na presença da tensão acústica é em geral diferente da situação em que temos o índice elipsóide em sua ausência. O campo muda as dimensões tanto quanto a orientação do índice elipsóide. Existem tabelas que ilustram, separadamente, a disposição e a magnitude dos coeficientes p_{qr} para diversos cristais [4,12-14]. Nestas tabelas, a simetria determina quais dos 36 coeficientes (matriz 6x6) são zeros, assim como a relação que pode existir entre os coeficientes matriciais que não são nulos.

2.3.1 Difração de Bragg em Meios Anisotrópicos

Muitas das características da difração da luz pelo som podem ser deduzidas se tomarmos vantagem da natureza dual onda-partícula da luz e do som. De acordo com este quadro, o feixe de luz com vetor de propagação **k** e freqüência ω pode ser considerado como um trem de partículas (fótons) com momento $\hbar\mathbf{k}$ e energia $\hbar\omega$. De modo semelhante, a onda

sonora pode ser considerada como sendo constituída de um trem de partículas (fônons) com momento $\hbar\mathbf{K}$ e energia $\hbar\Omega$. A difração da luz pela onda sonora pode então ser descrita como a soma de simples colisões, cada uma envolvendo a aniquilação de um fóton e um fônon incidente e a criação simultânea de um novo fóton difratado com freqüência $\omega'=\omega+\Omega$, que se propaga ao longo da direção do feixe espalhado. A conservação do momento requer que o momento $\hbar(\mathbf{k}+\mathbf{K})$ das partículas que colidem seja igual ao momento $\hbar\mathbf{k'}$ do fóton espalhado, de modo que $\mathbf{k'} = \mathbf{k}+\mathbf{K}$.

Em um meio isotrópico, o índice de refração associado com um feixe de luz é independente da direção de propagação e, portanto $|\mathbf{k'}|$ é com freqüência, quase o mesmo que $|\mathbf{k}|$. Faz-se necessário analisar um pouco as implicações disso. Seja *z* o eixo de direção de propagação de uma onda sonora e *yz* o plano coordenado paralelo ao plano de incidência. Se a dimensão transversa da onda acústica é infinita, as condições cinéticas de fronteira requerem que o feixe refletido permaneça no plano de incidência [3] (plano *yz*) com um ângulo de reflexão igual ao de incidência, θ. De acordo com a teoria do modo acoplado, a condição de ressonância nos dizia que

$$\beta_k - \beta_l - m\frac{2\pi}{\Lambda} = 0 \qquad (2.3.6)$$

para algum inteiro *m*. Esta condição também é conhecida como condição de Bragg[19]. No caso em que uma onda incidente seja representada por uma onda plana com um fator de propagação espacial dado por $\exp(-ik_y y - i\beta z)$, o acoplamento ocorre de forma forte com uma onda refletida com um fator de propagação espacial dado por $\exp(-ik_y y + i\beta z)$. A constante β é a componente do vetor de onda perpendicular aos planos relevantes do cristal. Segue, portanto, da equação (2.3.6) que o espaçamento entre os planos cristalinos Λ precisa satisfazer

$$\beta - (-\beta) = 2\beta = m\frac{2\pi}{\Lambda}$$

(2.3.7)

ou, uma vez que $\beta = k\cos\theta$, onde θ é o ângulo de incidência,

[19] Devido seu análogo na difração de cristais por Raios-X.

$$2\Lambda \cos \theta = m\lambda \ , \qquad (2.3.8)$$

onde m =1,2,3, ... é algum inteiro que corresponde ao m-ésimo componente de Fourier da perturbação dielétrica.

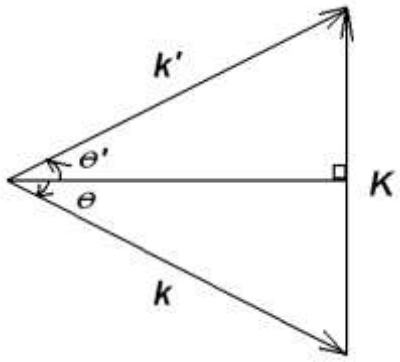


FIGURA 2.4: Representação da conservação do momento na difração de Bragg em um meio anisotrópico.

Vimos que a difração de luz por ondas sonoras pode ser expressa como uma interação entre três partículas o fóton incidente, um fônon acústico e o fóton difratado. A conservação do momento requer que os três vetores de momento associados com essas três partículas formem um triângulo. Em um meio anisotrópico, o índice relativo associado com o feixe de luz é, em geral, dependente da direção de propagação. Uma vez que o feixe de luz difratado, em geral, se propaga em uma direção diferente o feixe incidente, as magnitudes dos vetores de onda nem sempre são as mesmas. Em alguns casos, chega mesmo a existir mudanças no estado de polarização do feixe difratado. Sejam n' e n os índices de refração associados com os feixes difratado e incidente, respectivamente. O triângulo formado por **k**' e **K** possui lados iguais, respectivamente, a $n'\omega'$/c, $n\omega$/c, e **K** (veja FIGURA 2.4).

Uma vez que n' e n não são iguais, tal triângulo não é isósceles; mesmo se negligenciarmos pequenas diferenças entre ω e ω'. Sejam θ e θ' os ângulos entre os feixes de luz e a frente de onda da onda sonora (veja FIGURA 2.5).

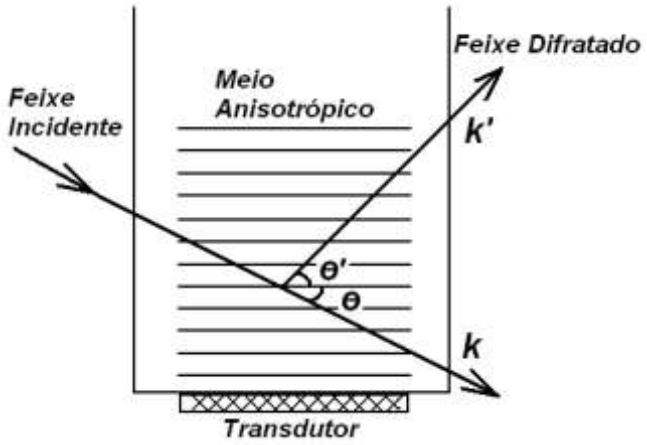


FIGURA 2.5: Difração de uma onda de luz por uma onda sonora na difração de Bragg em um meio anisotrópico.

A condição de Bragg, obtida do triângulo acima, nos diz que:

$$2\,k\,sen\;\theta = K - \frac{k'^2 - k^2}{K} \tag{2.3.9}$$

e

$$2\,k'\,sen\;\theta' = K + \frac{k'^2 - k^2}{K}, \tag{2.3.10}$$

ou ainda equivalentemente,

$$2\,\Lambda\,sen\;\theta = \frac{\lambda}{n} - \frac{\Lambda^2}{n\lambda}(n'^2 - n^2) \tag{2.3.11}$$

e

$$2\,\Lambda\,sen\;\theta' = \frac{\lambda}{n'} - \frac{\Lambda^2}{n'\lambda}(n'^2 - n^2)\,. \tag{2.3.12}$$

Para $n'=n$, a condição de Bragg é obtida novamente quando $\theta'=\theta$.

2.3.2 Análise dos Modos Acoplados na Difração de Bragg

A presente seção tenta demonstrar como se obter as intensidades e os estados de polarização dos feixes difratados. O formalismo do modo acoplado será agora empregado para estudar a difração de Bragg da luz por ondas sonoras. Fazendo isso, assumimos que a onda acústica é uma onda plana de extensão infinita, de tal modo que difrações de ordens mais altas são desprezadas e as únicas duas ondas acopladas pelo som são a incidente em ω e

a difratada em ω+Ω ou ω – Ω, dependendo da direção de propagação da onda sonora relativa ao feixe óptico incidente.

Por razões já discutidas, a onda sonora causa uma modificação na impermeabilidade dielétrica óptica dada por

$$\Delta \eta_{ij} = \Delta\left(\frac{\varepsilon_0}{\varepsilon}\right)_{ij} = p_{ijkl} S_{kl} \cos(\Omega t - Kz) \quad , \tag{2.3.13}$$

onde S_{kl} é a amplitude do trem de onda associado a onda sonora e z é a direção de propagação. Os termos p_{ijkl} são os coeficientes fotoelásticos. Somas sobre os índices repetidos *k* e *l* são assumidas. Tal modulação no tensor de impermeabilidade $\Delta\eta_{ij}$ corresponde a uma modulação em propagação no tensor dielétrico dada por

$$\Delta \varepsilon(z, t) = 2\varepsilon_1 \cos(\Omega t - Kz) \equiv \Delta\varepsilon \cos(\Omega t - Kz) \quad , \tag{2.3.14}$$

onde ε_1 é também um tensor e é expresso por $-\varepsilon(pS)\varepsilon / 2\varepsilon_0$, onde (*pS*) é a matriz com elementos $p_{ijkl}S_{kl}$. O fator 2 é inserido na equação (2.3.14) por conveniência, de tal forma que ε_1 é o primeiro (e único) coeficiente de Fourier da perturbação dielétrica Δε. Sobre condições apropriadas a perturbação dielétrica periódica acoplará os dois modos de propagação: a onda incidente e a onda difratada.

A equação que descreve a propagação do campo elétrico total dos dois modos acoplados, onda incidente e onda difratada, é dada por

$$\vec{E} = A_1 \vec{E}_1 \exp[i(\omega_1 t - k_1 r)] + A_2 \vec{E}_2 \exp[i(\omega_2 t - k_2 r)] \, . \tag{2.3.15}$$

Nesta equação, o índice 1 faz referência a luz incidente e o índice 2 a luz difratada. Desta forma ($\mathbf{k}_1$, $\mathbf{k}_2$) são os vetores de onda, ($\mathbf{E}_1$, $\mathbf{E}_2$) os vetores campo elétrico dos modos propagantes, (ω_1, ω_2) as respectivas freqüências, **r** é vetor que determina a posição espacial do campo elétrico e (A_1, A_2) são as amplitudes modais complexas. Na presença da perturbação dielétrica (2.3.14), ambas as amplitudes são funções da posição espacial. A dependência

temporal das amplitudes é desprezada, uma vez que Ω é muito menor em comparação com ω_1, e ω_2 e a perturbação dielétrica é praticamente estacionária[20].

Seja o plano de incidência (aquele formado por $\mathbf{k}_1$ e $\mathbf{K}$) o plano *xz*. A conservação do momento requer que $\mathbf{k}_2$ deve estar neste mesmo plano. O campo elétrico pode ser escrito como:

$$\vec{E} = A_1 \vec{E}_1 \exp\left[i(\omega_1 t - \alpha_1 x - \beta_1 z)\right] + A_2 \vec{E}_2 \exp\left[i(\omega_2 t - \alpha_2 x - \beta_2 z)\right] , \qquad (2.3.16)$$

em que $\beta_{1,2}$ são as componentes *z* dos vetores de onda $\mathbf{k}_1$ e $\mathbf{k}_2$, respectivamente, e $\alpha_{1,2}$ são as componentes destes vetores na direção *x* (paralelas às frentes de onda acústica). Para o problema bidimensional, as amplitudes A_1 e A_2 são funções de ambos *x* e *z*.

Contudo, há um número de casos no qual a configuração de interação requer que as amplitudes A_1 e A_2 sejam funções ambos de *x* e *z* apenas. A interação acústico-ótica é assim dividida em duas configurações de interação, ilustradas na FIGURA 2.6. Para baixas freqüências da onda sonora, a configuração apresentada na FIGURA 2.6(a) se aplica com mais freqüência; para altas freqüências, se aplica melhor à FIGURA 2.6(b). Em configurações com difração de Bragg para pequenos ângulos (FIGURA 2.6(a)), as amplitudes A_1 e A_2 são funções de *x* como requerido pelas condições de fronteira. Em configurações com difração de Bragg para grandes ângulos (FIGURA 2.6(b)), as amplitudes A_1 e A_2 são funções de *z* apenas[21]. Em ambos os casos, o campo elétrico deve satisfazer a equação de onda:

$$(\nabla^2 + \omega^2 \mu\varepsilon + \omega^2 \mu \Delta\varepsilon)\vec{E} = 0 \qquad (2.3.17)$$

onde ε é o tensor dielétrico do meio na ausência da onda sonora e Δε é a perturbação dielétrica devido ao som. Tanto $\vec{E}_1 \exp\left[i(\omega_1 t - \alpha_1 x - \beta_1 z)\right]$ quanto $\vec{E}_2 \exp\left[i(\omega_2 t - \alpha_2 x - \beta_2 z)\right]$ são soluções da equação (2.3.17) quando Δε = 0.

Substituindo a equação (2.3.15) em (2.3.16), tem-se

[20] As freqüências sonoras de interesse estão abaixo de 10^{10} THz, enquanto que as freqüências ópticas geralmente estão acima de 10^{13} THz.

[21] Novamente faremos uso da informação de que os filtros acústico-ópticos empregarem geralmente interação codirecional com grandes ângulos para pouparmos o leitor de uma exposição sobre a difração em pequenos ângulos. Mais uma vez, ao leitor interessado, indicamos a referência [3].

$$\sum_{m=1,2} \left\{ \left[\frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial z^2} - 2i\beta_m \frac{\partial}{\partial z} - 2i\alpha_m \frac{\partial}{\partial x} \right] A_m \right\} E_m \exp[\, i(\omega_m t - \alpha_m x - \beta_m z)$$

$$= -\omega^2 \mu \sum_{l=1,2} \Delta\varepsilon A_l \vec{E}_l \exp[\, i(\omega_l t - \alpha_l x - \beta_l z)]$$

(2.3.18)

As derivadas segundas podem ser desprezadas uma vez que a perturbação acústico-óptica é normalmente pequena ($\Delta\varepsilon/\varepsilon_0 \sim 10^{-5}$), e a equação (2.3.18) é dominada pelas derivadas primeiras. Entretanto, mesmo equações diferenciais de primeira ordem são difíceis de serem resolvidas em duas dimensões. Devemos então limitar nossa explanação aos casos mais comuns, mostrados na FIGURA 2.6, quando as equações diferenciais tornam-se unidimensionais.

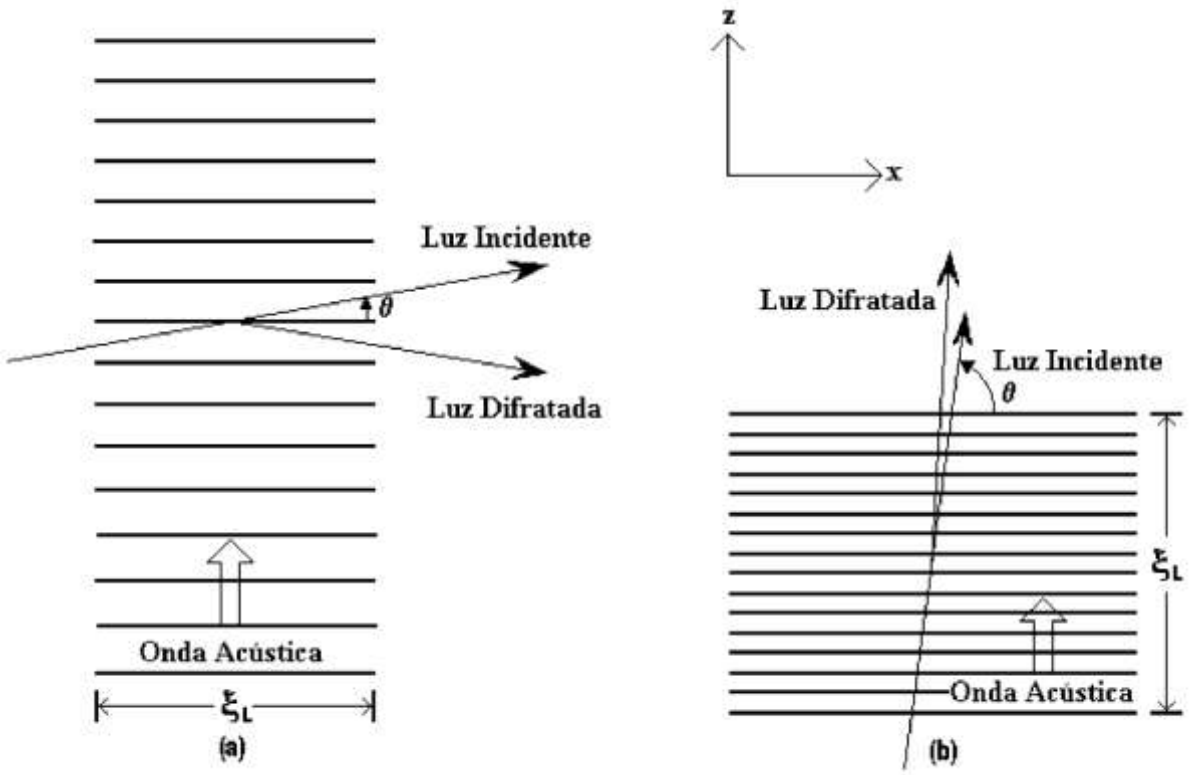


FIGURA 2.6: Os dois tipos de configurações comuns em uma interação acústico-óptica: (a) pequeno ângulo de incidência; (b) grande ângulo de incidência.

2.3.3 Difração de Bragg para Grandes Ângulos

As condições de contorno requerem que $\alpha_1 = \alpha_2$ na equação (2.3.16), e A_1 e A_2 são funções apenas de *z*. Além disso, o meio torna-se homogêneo nas direções *x* e *y*. Assim, o campo elétrico pode ser escrito como

$$\vec{E} = \left\{ A_1(z)\vec{E}_1 \exp\left[i(\omega_1 t - \alpha_1 x - \beta_1 z) \right] + A_2(z)\vec{E}_2 \exp\left[i(\omega_2 t - \alpha_2 x - \beta_2 z) \right] \right\} \exp(-i\alpha x), \quad (2.3.19)$$

onde β_1 e β_2 são as componentes *z* dos vetores de onda e α é a componente do vetor de onda paralelo a frente de onda da onda sonora. Os vetores $\vec{E}_1$ e $\vec{E}_2$ são normalizados de tal forma que

$$\vec{E}_i = \left(\frac{2\mu\omega_i}{|\beta_i|} \right)^{1/2} \vec{p}_i, \quad i = 1,2, \quad (2.3.20)$$

onde $\vec{p}_i$ são os vetores unitários descrevendo os estados de polarização dos modos. Com esta normalização, cada modo representa um fluxo de potência de 1 W/m^2 na direção *z* para o caso de um meio isotrópico. Uma vez que as freqüências acústicas de interesse são, em geral, muito baixas em relação às freqüências ópticas, tem-se pela lei de conservação da energia que $\omega_1 \approx \omega_2 = \omega$. Considerando tudo isso, a equação (2.3.18) pode ser simplificada e teremos apenas

$$\sum_{m=1,2} 2i\beta_m \frac{\partial A_m}{\partial z} E_m \exp(-i\beta_m z) = \omega^2 \mu \sum_{l=1,2} \Delta\varepsilon A_l \vec{E}_l \exp(-i\beta_l z). \quad (2.3.21)$$

A equação (2.3.21) constitui um par de equações diferenciais lineares acopladas, mas ainda não representa a forma utilizável para o estudo do AOTF neste trabalho, pois, apesar de descrever as variações das amplitudes modais com respeito somente a distância *z*, há a necessidade de se remover qualquer dependência espacial e temporal em relação à polarização transversal dos vetores $\mathbf{E}_1$ e $\mathbf{E}_2$ e a perturbação $\Delta\varepsilon$. Com este intuito, faz-se o produto interno dessa equação com $\mathbf{E}_l^* \exp(i\beta_l z)$. Em seguida, integra-se ao longo da seção transversal (*x*, *y*) e

sobre todo o tempo *t*. No final desse processo, as equações do modo acoplado obtidas para este caso são[22]:

$$\frac{dA_1}{dx} = -i\frac{\beta_1}{|\beta_2|}\kappa_{12} A_2 \exp(-i\Delta\beta z), \tag{2.3.22}$$

$$\frac{dA_2}{dx} = -i\frac{\beta_2}{|\beta_2|}\kappa_{12}^{*} A_1 \exp(-i\Delta\beta z), \tag{2.3.23}$$

onde $\Delta\beta$ é a diferença de fase longitudinal, dada por

$$\Delta\beta = \beta_1 - \beta_2 \pm K;$$

(2.3.24)

e κ_{12} é constante de acoplamento entre os dois modos de propagação, dada por

$$\kappa_{12} = \frac{\omega^2\mu}{2\sqrt{|\beta_1\beta_2|}}\vec{p}_1^{*}\cdot\varepsilon_1\vec{p}_2. \tag{2.3.25}$$

Estas são duas das variáveis mais importantes para o estudo AOTF.

2.3.4 Acoplamento Codirecional ($\beta_1\beta_2>0$)

Como já foi dito algumas vezes, geralmente um AOTF utiliza acoplamento codirecional. Isso se dá porque em um acoplamento contradirecional as freqüências acústicas requeridas são excessivamente altas, o que impossibilita sua propagação em muitos sólidos. No acoplamento codirecional (veja FIGURA 2.7), a onda propagada (A_2) e a incidente (A_1) estão na mesma direção (ambas em +*z* ou – *z*). Essas duas ondas são acopladas e suas propagações características são descritas pelas equações (2.3.22) e (2.3.23). Sejam, então, $\theta_{1,2}$ os ângulos entre os vetores de onda $k_{1,2}$ e frente de onda acústica, e usando (2.3.14) e $\varepsilon_1 = -\varepsilon(pS)\varepsilon/2\varepsilon_0$, temos:

[22] Nesta passagem, alguns passos foram omitidos. Entretanto, um leitor interessado na dedução completa pode encontrá-la na referência [15].

$$\kappa_{12} = \frac{\omega \vec{p}_1^{\,*} \cdot \varepsilon'(pS)\varepsilon' \vec{p}_2}{4c\sqrt{\left|n_1 n_2 \operatorname{sen}\ \theta_1 \operatorname{sen}\ \theta_2\right|}}, \tag{2.3.26}$$

onde $n_{1,2}$ são os índices de refração associados com as ondas, $\vec{p}_{1,2}$ são os estados de polarização e S é o tensor da perturbação mecânica.

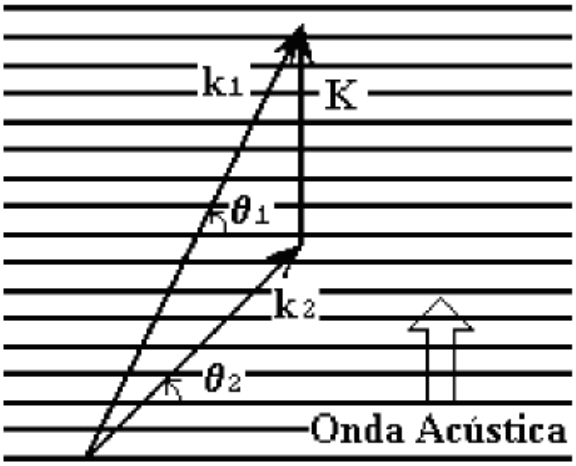


FIGURA 2.7: Acoplamento codirecional entre a luz incidente e a difratada ($\beta_1\beta_2 > 0$).

A solução geral para as equações (2.3.22) e (2.3.23), para o caso de uma única onda incidente em $z = 0$, com $A_1 = \text{const}$ e $A_2 = 0$ é:

$$A_1(z) = A_1(0)e^{i\frac{1}{2}\Delta\beta z}\left[\cos\ sz - i\frac{\Delta\beta}{2s}\operatorname{sen} sz\right] \tag{2.3.27}$$

$$A_2(z) = -iA_1(0)e^{-i\frac{1}{2}\Delta\beta z}\frac{\kappa_{12}^{*}}{s}\operatorname{sen} sz \tag{2.3.28}$$

onde

$$s^2 = \left|\kappa_{12}\right|^2 + \left(\frac{1}{2}\Delta\beta\right)^2. \tag{2.3.29}$$

A inspeção desta solução revela que a potência transferida entre os dois modos é máxima quando $\Delta\beta = 0$. A fração de potência transferida durante uma distância de interação L é dada por

$$T = \frac{\left|A_2(L)\right|^2}{\left|A_1(0)\right|^2} = \frac{\left|\kappa_{12}\right|^2}{\left|\kappa_{12}\right|^2 + (\frac{1}{2}\Delta\beta)^2} sen^2 sL \quad . \tag{2.3.30}$$

2.4 Conclusão

Após obtermos as equações do modo acoplado para as ondas se propagando no interior do acústico-óptico, no capítulo que se segue iremos resolver essas equações através de métodos numéricos considerando as características físicas do meio em questão. Levaremos em consideração valores de perda e não linearidade e estudaremos o fenômeno da biestabilidade.

2.5 Referências Bibliográficas

[1] BRILLOUIN, Léon. Diffusion of Light and X-rays by a Transparent Homogeneous Body. Ann. Phys.**,** Paris, v. 17, p.88-122, 1922.

[2] DEBYE, P.; SEARS, F.w.. On the scattering of light by supersonic waves. Proc. Nat. Acad. Sci., Usa, n. 18, p.409-414, 1932.

[3] JACKSON, John David. Classical Eletrodinamics. New York: John Wiley & Sons, Inc., 1962.

[4] YARIV, Amnon; YEH, Pochi. Optical Waves in Crystals. New Jersey: John Wiley & Sons, Inc, 2003. (Wiley Classics Library).

[5] AGRAWAL, Govind P.; KAMINOW, Ivan P.; KELLEY, Paul L.. Nonlinear Fiber Optics. 3. ed. New York: Academic Press, 1995.

[6] WEBER, Marvin J.. Handbook of Optical Materials. California: Crc Press, 2003.

[7] ABELES, F.. Investigations on the propagation of sinusoidal electromagnetic waves in stratified media, apllication to thin films. Ann. Phys., v. 5, p.256-256, 1950.

[8] ABELES, F.. Investigations on the propagation of sinusoidal electromagnetic waves in stratified media, apllication to thin films II. Ann. Phys. v. 5, p.706-706, 1950.

[9] YEH, Pochi; YARIV, Amnon; HONG, C. S.. Electromagnetic propagation in periodic stratified media I, general theory. J. Opt. Soc. Am. v. 67, n. , p.423-437, 1977.

[10] YARIV, Amnon; YEH, Pochi. II Birefringence, phase matching, and X-ray lasers. J. Opt. Soc. Am., v. 61, p.438-448, 1977.

[10] YARIV, Amnon; YEH, Pochi; CHO, A. Y.. Optical surface waves in periodic layered media. Applied Physics Letters, v. 32, n. 2, p.104, 1978.

[11] YARIV, Amnon. Coupled-Mode Theory for Guided-Wave Optics. IEEE Journal Of Quantum Electronics, v. 9, n. 9, p.919-933, 1973.

[12] NEWNHAM, Robert Everest. Properties of materials: anisotropy, symmetry, structure. Oxford: Oxford University Press, 2005.

[13] LIU, Jia-ming. Photonic devices. Cambridge: Cambridge University Press, 2005.

[14] LIDE, David R.. CRC Handbook of Chemistry and Physics. Eua: Crc Press, 2006.

[15] SARAIVA SOBRINHO , Cícero. Estudo do desempenho de filtros acústico-ópticos sintonizáveis com não linearidade crescente e perdas para aplicações em redes ópticas de telecomunicações. 2002. 73 f. Dissertação (Mestrado) - Curso de Engenharia Elétrica, Departamento de Engenharia Elétrica, Universidade Estadual do Ceará, Fortaleza, 2002.

3 CARACTERIZAÇÃO E PROPRIEDADES DE UM AOTF

O capítulo anterior apresentou a teoria que explicava a interação acústico-óptica. Tal teoria nos possibilita construir dispositivos que utilizem esse efeito para selecionar as freqüências que se deseja permitir passar ou não por ele: são os filtros acústico-ópticos sintonizáveis. Antes de aplicarmos esses dispositivos no processo de codificação proposto nesse trabalho, dedicaremos o presente capítulo a um breve estudo sobre eles. Isso se justifica pela necessidade de conhecer o funcionamento do mesmo o mais precisamente possível, uma vez que este trabalho se baseia em simulações computacionais. Destarte, o algoritmo precisa ser testado comparando com resultados já conhecidos. Destacaremos nesse estudo, a análise que fizemos sobre o efeito de biestabilidade que encontramos em nossas simulações. Encontramos resultados bem significativos e achamos que o espaço seria adequado para expô-los.

3.1 Filtros Acústico-Ópticos Sintonizáveis

Basicamente, existem três tipos de dispositivos acústico-ópticos (AO): defletores, demoduladores e filtros sintonizáveis. Cada um deles pode usar diferentes tipos de interação entre luz e som. O tipo de interação AO é determinada pela geometria e pelas propriedades acústicas do material a compor o dispositivo. No entanto, todas as interações são baseadas no efeito fotoelástico e podem ser isotrópicas ou anisotrópicas, dependendo das propriedades do cristal. Interações isotrópicas não mudam a polarização do feixe óptico e podem resultar em feixes difratados de uma ou múltiplas ordens. A difração de uma única ordem isotrópica é chamada de Bragg. Por ser muito mais eficiente, é a que se usa na prática. Interações anisotrópicas mudam a polarização do feixe óptico e resultam numa difração de uma única ordem. Elas oferecem maior eficiência e maiores larguras de banda acústica e óptica que as isotrópicas. Defletores de alto desempenho e AOTF são geralmente baseados em interações anisotrópicas [1].

O AOTF já é comercializado e é utilizado em diversas áreas, como espectroscopias atômica [2,3], molecular[4], molecular florescente [5], Raman [6], telecomunicação [7,8], tecnologias com laser [9,10] e processamento de imagens [11-20]. Eles são sensíveis a polarização da luz incidente, uma vez que é necessário o uso de radiação linearmente

polarizada[23]. É importante ressaltar sua versatilidade em aplicações em redes de comunicações ópticas. O AOTF é, provavelmente, o único filtro capaz de selecionar múltiplos comprimentos de onda simultaneamente, pois um único cristal pode acomodar múltiplas ondas acústicas de freqüências diferentes. Seu princípio básico de operação pode ser usado para construir conexões cruzadas de múltiplos comprimentos de onda em redes WDM. As conexões cruzadas permitem uma arquitetura de rede reconfigurável, que possa se adaptar às mudanças no tráfico de informações [21]. A dificuldade que pode surgir neste tipo aplicação é o alto nível de *"crosstalk"* introduzido pelo dispositivo.

3.2 Esquema Geral

O esquema geral de um AOTF é mostrado na FIGURA 3.1. Ele consiste de um guia de onda acústico óptico suportando apenas os modos (TE e TM) de ordem mais baixa, isto é, existem apenas dois modos confinados no guia (TE_1 e TM_1). A radiofreqüência (RF), aplicada a um ***transdutor de onda acústica superficial*** (SAW), excita a onda acústica no ***guia de onda óptico*** determinando o ***comprimento de onda*** que será transmitido. O campo acústico atua sobre o campo óptico na região de interação convertendo a polarização TE para TM e vice-versa (TE $\leftrightarrow$ TM). Esta interação seleciona a freqüência, uma vez que requer o descasamento de fase para que a interação seja significativa. Como já discutimos matematicamente no capítulo anterior, a eficiência na conversão da polarização pode ser calculada tratando o dispositivo com um acoplador direcional clássico onde os modos acoplados são os modos TE e TM do guia de onda óptico [28].

No que concerne à fabricação do AOTF, dois fatores são cruciais: o tamanho e a forma do ***transdutor de onda acústica***. Eles influenciam diretamente nas propriedades do dispositivo, como, por exemplo, a resolução espectral (FWHM), a potência elétrica requerida para uma dada eficiência de difração, etc. [11,29]. Para a construção de AOTF com altas resoluções é preciso desenvolver uma célula acústico-óptica com um grande comprimento de interação. As células usadas rotineiramente têm a desvantagem de que o comprimento de interação é determinado pelo tamanho do transdutor piezelétrico [1]. Em adição, um grande transdutor tem alta capacitância e pequena resistência elétrica. Na tentativa de resolver esses problemas, geralmente usa-se a segmentação dos transdutores. Contudo, esse procedimento

[23] A comparação da eficiência entre o AOTF e outros filtros pode ser encontrada em [1].

resulta num complexo processo de construção e numa complexa combinação entre o transdutor piezelétrico e o gerador de sinal RF [30].

Os ***guias de ondas*** podem ser fabricados a partir de certo número de materiais inorgânicos, dielétricos ou semicondutores. Estes materiais incluem $LiNbO_3$, $LiTaO_3$, $KNbO_3$, KTP ($KTiOP_4$) e os semicondutores GaAs e InP. Atualmente, o material utilizado com maior freqüência é o $LiNbO_3$ [31]. O conhecimento dos aspectos fenomenológicos da tecnologia de fabricação de guias em $LiNbO_3$ é suficiente para confeccionar dispositivos com um desempenho satisfatório (baixas perdas, grandes larguras de banda e etc.) [32,33].

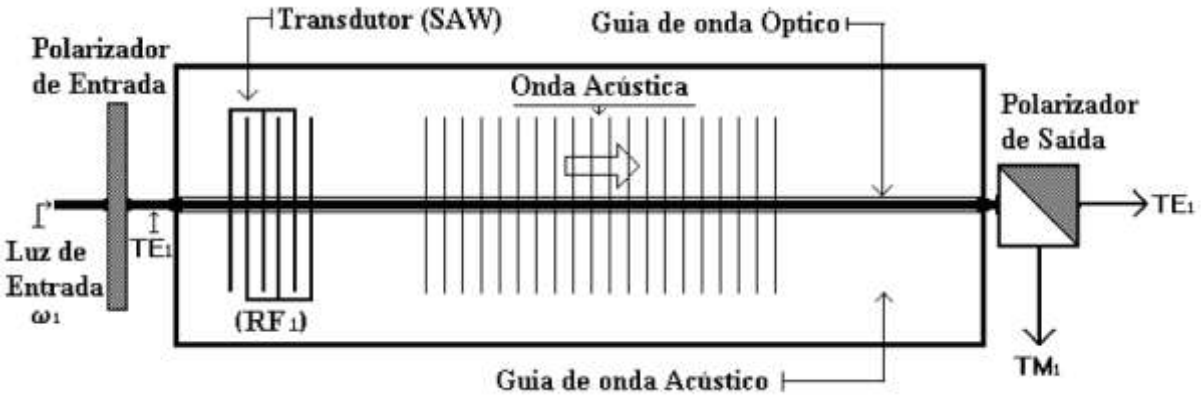


FIGURA 3.1: Esquema geral de um AOTF.

3.3 Características de Transmissão de um AOTF

Quando a energia da luz de entrada é polarizada em uma faixa estreita, no modo TE (indicado na FIGURA 3.1 por TE_1), por exemplo, em torno de uma dada freqüência escolhida, será convertida para o modo TM (indicada na FIGURA 3.1 por TM_1), enquanto o resto da energia permanece no modo TE [34-36]. Ainda na FIGURA 3.1, o polarizador, por sua vez, serve para separar os dois modos e pode ser externo ao dispositivo ou integrado sobre o cristal. Imperfeições no polarizador (PBS) podem resultar em perdas na eficiência de chaveamento, e contribuir para algum tipo de ***crosstalk***.

De uma forma geral, o AOTF permite um chaveamento simultâneo e independente de múltiplos comprimentos de onda (canais), escolhidos arbitrariamente e estreitamente espaçados, uma grande e flexível faixa de comprimentos de onda endereçados, rápida sintonia (da ordem de μs), baixa perdas ópticas (3 a 4 dB / estágio). Além disso, permite a integração

de várias funções no mesmo substrato do cristal. Recentes melhorias no seu projeto incluíram uma curva de transmissão mais plana e com a redução dos picos secundários[37], o que por sua vez reduz o ***crosstalk*** e aumenta a razão largura do canal/espaçamento entre canais.

Geralmente os AOTF empregam a interação codirecional com grandes ângulos. Forte interação acústico-óptica ocorre apenas quando a condição de Bragg é satisfeita. Se o feixe de luz incidente contém muitas componentes espectrais, apenas uma irá satisfazer a condição de Bragg em uma dada freqüência acústica. Em outras palavras, apenas uma componente espectral será difratada em uma dada freqüência acústica. Portanto, ao variarmos a freqüência acústica, a freqüência (ou comprimento de onda) do feixe difratado também pode ser variada. A fração da potência transferida do feixe incidente para o feixe difratado, por um comprimento de interação L, é dada pela equação (2.3.30):

$$T = \frac{sen^{2}\left[\kappa_{12} L \sqrt{1 + \left(\Delta\beta / 2\kappa_{12}\right)^{2}}\right]}{1 + \left(\Delta\beta / 2\kappa_{12}\right)^{2}}, \qquad (3.3.1)$$

onde κ_{12} é a constante de acoplamento, dada pela equação (2.3.25)

$$\kappa_{12} = \frac{\omega^{2}\mu}{2\sqrt{\left|\beta_{1}\beta_{2}\right|}} \vec{p}_{1}^{\,*} \cdot \varepsilon_{1} \vec{p}_{2},$$

e $\Delta\beta$ é a diferença de fase, dada pela equação (2.3.24):

$$\Delta\beta = \beta_{1} - \beta_{2} \pm K ;$$

β_1 e β_2 são as componentes do vetor de onda dos feixes incidente e refratado, respectivamente, ao longo da direção de propagação da onda acústica. Sejam θ_1 e θ_2 os ângulos dos vetores de onda medidos da frente de onda da onda sonora, de tal forma que

$$\beta_{1} = \frac{w}{c} n_{1} sen\ \theta_{1} = \frac{2\pi}{\lambda} n_{1} sen\ \theta_{1}, \qquad (3.3.2)$$

$$\beta_2 = \frac{w}{c} n_2 sen\ \theta_2 = \frac{2\pi}{\lambda} n_2 sen\ \theta_2 , \qquad (3.3.3)$$

onde n_1 e n_2 são os índices de refração associados com as ondas incidente e difratada respectivamente. A conservação do momento (condição de Bragg), $\Delta\beta = 0$, torna-se:

$$\frac{2\pi}{\lambda}(n_2 sen\ \theta_2 - n_1 sen\ \theta_1) = \pm \frac{2\pi}{v} f , \qquad (3.3.4)$$

onde f é a freqüência acústica e v é a velocidade do som no meio. A partir desta equação pode-se perceber que o número de onda ($2\pi/\lambda$) da luz difratada é proporcional a freqüência acústica f. Da equação (3.3.1), é possível observamos que a fração de potência transferida torna-se muito pequena quando $\Delta\beta >> \kappa$[24] e a máxima transferência só é possível na condição de Bragg (ou descasamento de fase), $\Delta\beta = 0$. É fácil de perceber que muito embora esta condição seja necessária, não é suficiente para que a transferência seja máxima (100%), uma vez que o argumento da função seno na equação (3.3.1) deve, para isso, ser igual a $\pi/2$. Isto implica em uma segunda condição para a máxima eficiência na conversão de potência entre os modos, dada por:

$$\kappa L = \frac{1}{2}\pi , \qquad (3.3.5)$$

Substituindo (3.3.5) em (3.3.1), agora não necessariamente na condição de Bragg, teremos a transmissão de potência em função de $\Delta\beta L$:

$$T = \frac{sen^2\left[\frac{\pi}{2}\sqrt{1 + (\Delta\beta L/\pi)^2}\right]}{1 + (\Delta\beta L/\pi)^2} . \qquad (3.3.6)$$

Um cálculo rápido mostra que a eficiência da conversão cai para 50% (T = 0,5) quando $\Delta\beta L \cong \pm 0{,}80\pi$. L é comprimento da região onde ocorre a interação entre o campo acústico e o óptico.

[24] Para facilitar a exposição dos gráficos, substituiremos daqui em diante o termo κ_{12} por κ apenas. O significado físico permanecerá o mesmo.

Isto corresponde a uma largura de banda (FWHM) total da curva de transmissão, de acordo com esse resultado e com a equação (3.3.4), de

$$\Delta\lambda_{1/2} = \frac{0.8\lambda^2}{\left|n_2 sen\ \theta_2 - n_1 sen\ \theta_1\right| L} \tag{3.3.7}$$

que, para o caso colinear ($\theta_1 = \theta_2 = \pi/2$), reduz-se a [38]

$$\Delta\lambda_{1/2} = \frac{0.8\lambda^2}{\left|\Delta n\right| L}. \tag{3.3.8}$$

No modelo para o AOTF em nossas simulações, o produto $\Delta\beta\xi_L$ é considerado constante para o mesmo T e Δn depende do meio que o dispositivo é constituído.

3.3.1 Procedimento Experimental

Inicialmente analisaremos as curvas de transmissão de um AOTF linear e ideal em função dos seus parâmetros, a saber, o comprimento L, constante de acoplamento, κ, e o descasamento de fase, $\Delta\beta$. Para isso, usamos inicialmente ondas contínuas no tempo (CW), definindo as condições de contorno $A_1(0) = 1$ (constante) e $A_2(0) = 0$.

Para resolver as equações acopladas, levando em consideração essas condições de contorno, utilizamos o método numérico de Runge-Kutta de Quarta Ordem [39-41]. Construímos, para esta simulação inicial, uma janela temporal de 100ps a partir de 1024 pontos. Ainda para esse estudo, consideramos nulo o coeficiente de perda no dispositivo.

Usamos pulsos ultracurtos com largura temporal de Δt_{pulso} = 2 ps. Mas na prática é costume se usar a largura à meia altura (FWHM), de tal forma que Δt_0 = 1.135ps[25] [42]. O comprimento do AOTF usado foi de aproximadamente L = 2,18 mm usando o valor de parametrização Δn = 0.07 para a birrefringência induzida no material. Os coeficientes de

[25] Uma vez que para pulsos secante-hiperbólicos, como no caso de pulsos sólitons, temos que:
$T_{FWHM}=2\ln(1+\sqrt{2})T_0 \approx 1.763\ T_0$.

dispersão de segunda ordem e não-linearidade são dados por $\beta^{(2)} = -0.127\times 10^{-27}$ ps^2/mm e $\gamma = 0.098\times10^{-3}$ (W mm)$^{-1}$, respectivamente. O valor básico para a potência é P_0=1W.

3.2.2 Curvas de Transmissão

Assim, a eficiência na conversão na transmissão do filtro, T, em uma dada freqüência acústica pelo desvio normalizado na freqüência óptica, $\Delta\beta L$, é mostrada na Figura 3.2. Pode-se facilmente observar que a curva só atinge o valor máximo para a curva $\kappa L=\pi/2$ com $\Delta\beta L=0$ (condição de Bragg).

A potência elétrica aplicada ao transdutor é proporcional a intensidade acústica requerida para a conversão de modos. Entretanto, existe uma perda (na conversão elétrico-acústica) na interface entre o cristal e o transdutor, o que implica no aquecimento do cristal. Como resultado disto 100% de conversão, entre os modos, torna-se difícil de alcançar em um AOTF. A variação do parâmetro κL pode refletir muito bem este comportamento. O desvio no valor de κL, a partir da condição de máxima transmissão de pico, resulta em uma correspondente variação na banda e intensidade da curva de transmissão do filtro.

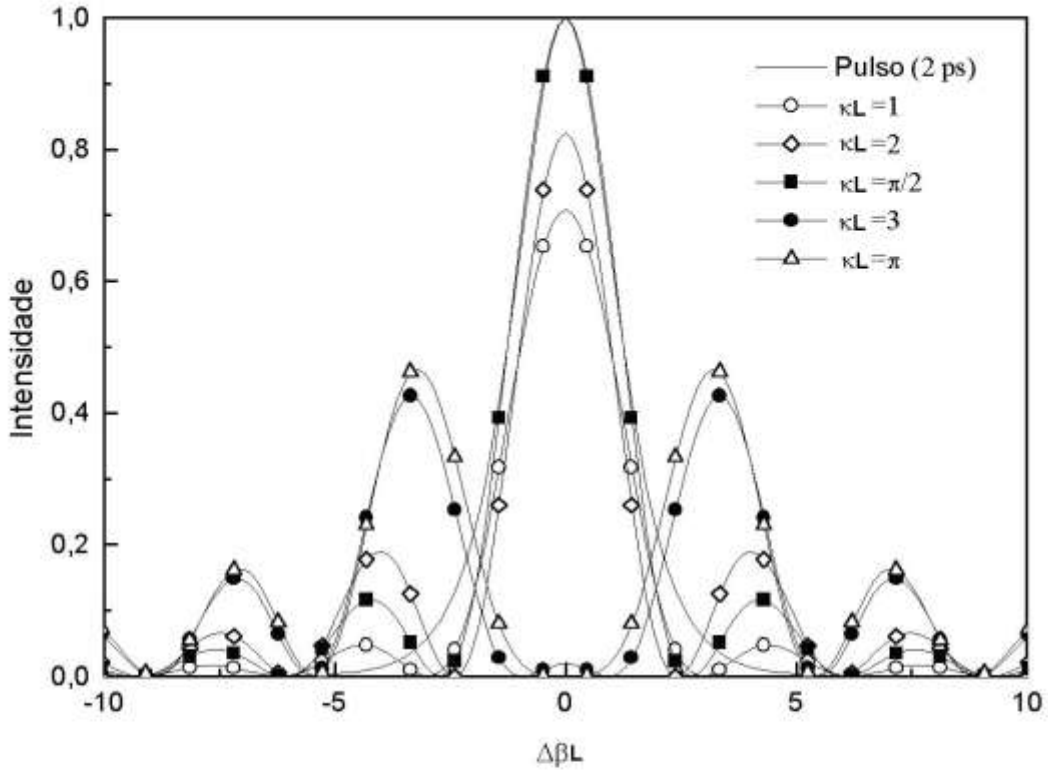


FIGURA 3.2: Comparações de intensidade e largura de banda entre o coeficiente de transmissão (*T*) para um pulso de 2 ps (0,157 THz), para diferentes valores do produto κL (Fonte: Ref. [44]).

A FIGURA 3.3 mostra o espectro do pulso para quatro comprimentos diferentes do dispositivo. Estamos considerando o valor de referência como sendo L = 2,18 mm, como dito anteriormente, e os demais valores analisados foram ξ_L = *L/10*, *L/3* e *3L*. Observa-se dessa figura que o acréscimo no comprimento ξ_L corresponde a um estreitamento na banda de freqüências que o filtro permitirá passar. Um AOTF colinear não possui grande largura de banda óptica [43].

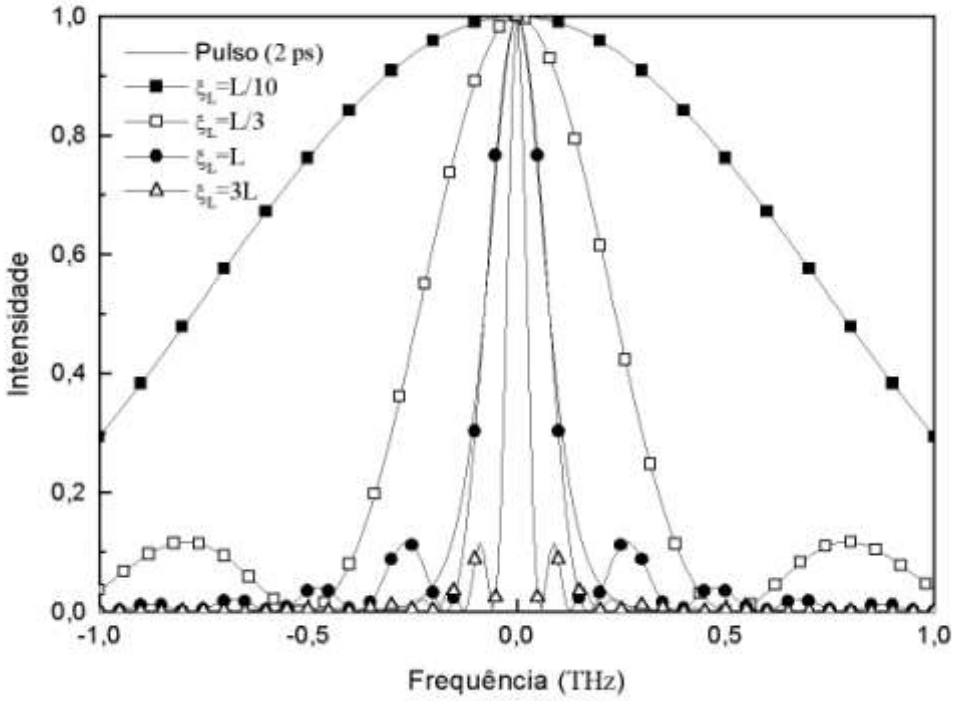


FIGURA 3.3: Comparação entre a largura de banda de um AOTF e um pulso de 2 ps (0,157 THz), para quatro comprimentos diferentes do dispositivo, com $\kappa\xi_L = \pi/2$ (fixo) (Fonte: Ref. [44]).

Interessantes estudos foram realizados sobre os efeitos de não-linearidades e perda sobre essas curvas de transmissão [7,44]. Na seção seguinte apresentaremos um pequeno resumo sobre eles e os resultados obtidos.

3.4 Perfis de Não-Linearidade e Perda

Antes da invenção do ***laser***, acreditava-se que todo meio óptico era linear. Contudo, com seu advento, foi possível examinar o comportamento dos meios materiais submetidos a altas intensidades de luz. Surgiu então uma grande variedade de novos estudos e aplicações dentro da óptica não linear.

A linearidade (ou não-linearidade) é uma propriedade do meio através do qual a luz se propaga. A presença de um campo óptico modifica as propriedades do meio que, por sua vez, pode modificar outro campo óptico ou o próprio campo original. No caso do AOTF, funcionando num regime não-linear, a potência óptica aplicada na entrada dispositivo, em uma dada freqüência, é transferida a um conjunto de outras freqüências. O campo óptico perturba os átomos do material, mudando o índice de refração do meio e provocando vários processos de espalhamento[26] [7].

3.4.1 Propagação Eletromagnética em Meios Não-Lineares

No desenvolvimento das equações acopladas para o AOTF (linear), não foram considerados os possíveis efeitos que surgem como resposta aos campos eletromagnéticos intensos. A permissividade dielétrica (Equação 2.1.29), não incluiu os termos que descrevem a polarização do meio devido ao tensor de susceptibilidade elétrica χ. Para incluir os efeitos de não-linearidade é preciso encontrar o termo a ser adicionado as equações do modo acoplado já obtidas.

A polarização total ($\mathbf{P}_T$) pode ser escrita como a soma $\mathbf{P}_T = \mathbf{P} + \mathbf{P}_P$, em que $\mathbf{P}_P$ é o desvio de polarização devido à perturbação dielétrica. A polarização induzida no meio deixa de ser proporcional ao campo elétrico e passa a satisfazer a uma relação mais geral:

$$\mathbf{P} = \varepsilon_0 (\chi^{(1)} \otimes \mathbf{E} + \chi^{(2)} \otimes \mathbf{EE} + \chi^{(3)} \otimes \mathbf{EEE} + \dots). \qquad (3.4.1)$$

onde $\chi^{(m)}$ (m = 1, 2, 3 ...) é o tensor de susceptibilidade elétrica (ordem m) do meio dielétrico. Em geral[27], a polarização **P** pode ser dividida em duas partes, uma linear e outra não linear ($\mathbf{P} = \mathbf{P}_L + \mathbf{P}_{NL}$) [45]:

---

[26] Em baixas intensidades, o espalhamento é uma função linear do campo aplicado e é conhecido como Espalhamento de Rayleigh, o qual resulta de uma perturbação descrita por um índice de refração constante. Espalhamentos inelásticos resultam de intensidades maiores, as quais provocam perturbações que não são mais funções lineares do campo aplicado. Neste tipo de espalhamento surgem efeitos não lineares conhecidos como Efeito Kerr, Espalhamento de Raman e Espalhamento de Brillouin.

[27] A polarização elétrica de um dado meio material deve trazer embutidas todas as propriedades elétricas do meio, assim como a magnetização deve conter as propriedades magnéticas. Estas duas grandezas constituem a resposta do meio aos campos externos.

$$\mathbf{P}_{L} = \varepsilon_0 \chi^{(1)} \otimes \mathbf{E}$$
$$\mathbf{P}_{NL} = \varepsilon_0 (\chi^{(2)} \otimes \mathbf{EE} + \chi^{(3)} \otimes \mathbf{EEE} + \dots). \qquad (3.4.2)$$

A susceptibilidade linear $\chi^{(1)}$ representa a contribuição dominante para a polarização **P**, sendo que seus efeitos estão inclusos no índice de refração linear n_L e no coeficiente de atenuação α do meio. As susceptibilidades de segunda e terceira ordem $\chi^{(2)}$ e $\chi^{(3)}$ são responsáveis pelo comportamento não linear. Em particular, $\chi^{(2)}$ provoca efeitos não lineares como geração de segundo harmônico, geração de soma e diferença de freqüências, etc. Para o estudo do AOTF não-linear, será suposto que o termo $\chi^{(2)}$ é desprezível[28]. Assim, o comportamento não-linear do meio será apenas devido ao termo de susceptibilidade $\chi^{(3)}$. A parte real de $\chi^{(3)}$ é responsável pelo Efeito Kerr[29]. O efeito Kerr é o fenômeno no qual o índice de refração do meio muda quando a órbita do elétron é deformada por um forte campo elétrico [46].

A não-linearidade Kerr dá origem a diferentes efeitos, dependendo das condições com que o sinal óptico é bombeado no guia. Dentre eles estão a automodulação de fase (SPM), a modulação cruzada de fase (XPM), a instabilidade modulacional e outros processos paramétricos tais como geração de harmônicos, amplificação paramétrica e mistura de quatro ondas [42]; efeitos, estes, usados nas mais diversas aplicações, como chaveamento óptico, portas lógicas, compressão de pulsos, computação óptica, etc..

O termo SPM refere-se a uma mudança de fase auto-induzida experimentada por um pulso óptico durante sua propagação em um meio dielétrico. A magnitude desta mudança pode ser obtida observando que a fase do campo óptico muda através de

$$\phi = \frac{n \omega_o L}{c} = \frac{(n_L + n_{NL} I) \omega_o L}{c}, \qquad (3.4.3)$$

[28] Com esta simplificação não existe perda de generalização, pois este termo é diferente de zero somente para meios sem uma inversão de simetria a nível molecular. No caso de fibras ópticas, compostas por moléculas simétricas de SiO_2, ele é sempre nulo. A susceptibilidade de terceira ordem $\chi^{(3)}$ é responsável por fenômenos tais como geração de terceiro harmônico e efeito Kerr.
[29] E a parte imaginária pelo Efeito Raman.

em que $\omega_o=2\pi f_o$, L é o comprimento propagado, n_L é a parte linear do índice de refração do meio e n_{NL} é a parte não linear. Portanto, $\phi_{NL}=(n_{NL}I\omega_oL)/c$ é a mudança de fase não linear devido a SPM.

Pode-se mostrar que o perfil $A(z,t)$ de um pulso ultracurto propagando-se no meio considerado, deve satisfazer a seguinte equação diferencial não linear [44]

$$\frac{\partial A}{\partial z} = i\gamma \,|A|^2\, A\,, \qquad (3.4.4)$$

em que $\gamma = \frac{\omega_o n_{NL}}{2cZ_I}$ é um coeficiente representando o efeito não linear. Esta equação permite a solução $A(z,t) = A(0,t)\exp[i\phi_{NL}(z,t)]$, em que $\phi_{NL}(z,t) = \gamma z|A(0,t)|^2$. Apesar de $\phi_{NL}(z,t)$ ter uma dependência temporal, é possível verificar que o pulso propagado mantém o perfil de sua intensidade temporal, ou seja, $|A(z,t)|^2 = |A(0,t)|^2$. Portanto, antes de fazer a modelagem matemática para o AOTF não-linear básico, convém fazer uma rápida análise sobre o efeito de $\phi_{NL}(z,t)$ no perfil espectral do pulso propagado.

Na prática, o termo ϕ_{NL} causa um ***chirp*** não-linear no campo transmitido. Na ausência da dispersão de velocidade de grupo (GVD), a presença de um ***chirp*** não-linear causa o alargamento espectral (em freqüência) do sinal. Este alargamento espectral é uma conseqüência da dependência temporal de ϕ_{NL} e depende do perfil do pulso considerado, pois, $\phi_{NL}(z,t) = \gamma z|A(0,t)|^2$. O ***chirp*** não-linear, induzido pela SPM, cresce em magnitude com a distância propagada z. Em outras palavras, novas componentes de freqüência são continuamente geradas à medida que o pulso se propaga no meio.

As curvas da FIGURA 3.4 foram obtidas da equação (3.4.4) como uma função do máximo valor de ϕ_{NL}, o qual ocorre no centro do pulso e é dado por $\phi_{NLmáx} = \gamma P_0 L = L / L_{NL}$. Note que $L_{NL} = (\gamma P_0)^{-1}$, é o comprimento de não-linearidade e P_0 é a potência inicial do pulso. O significado físico de L_{NL} torna-se evidente quando $\phi_{NLmáx} = 1$, pois, neste caso L_{NL} é a própria distância propagada L. O pulso inicial, neste caso, possui perfil secante hiperbólico, sem nenhum ***chirp*** inicial, tendo uma duração temporal de 2 ps. O comportamento mais notável dessa figura é a presença de uma estrutura oscilatória em toda faixa de freqüência,

acompanhando o alargamento espectral. Em geral, o espectro consiste de muitos picos, sendo que os picos mais externos são mais intensos.

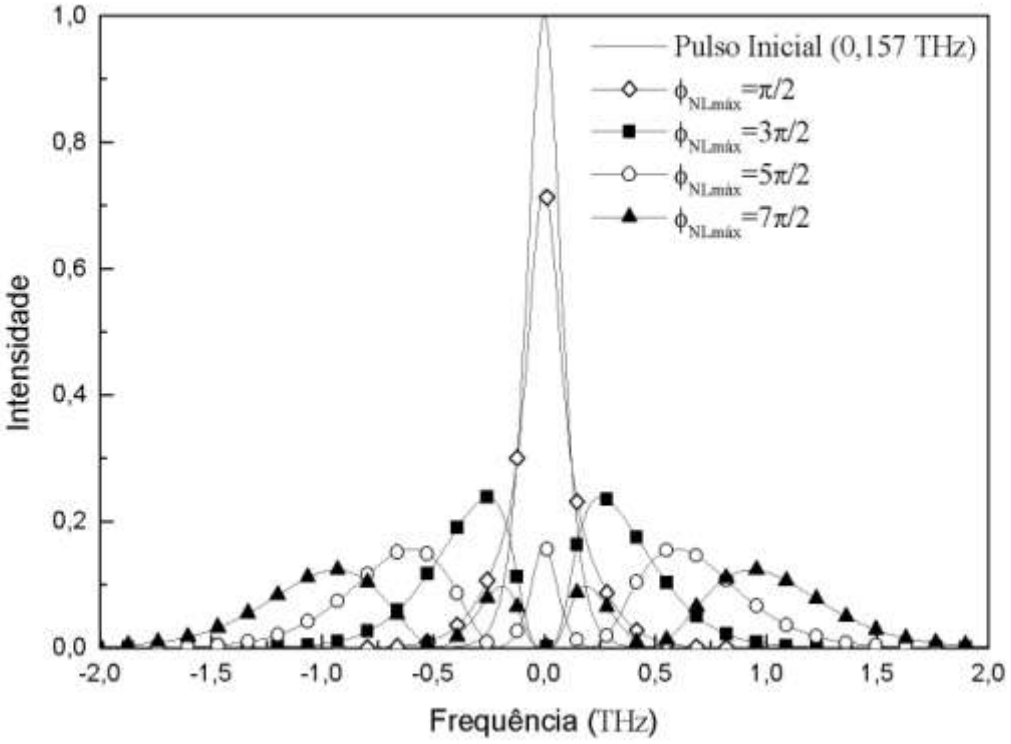


FIGURA 3.4: Alargamento espectral devido à auto modulação de fase (SPM), em relação à máxima mudança de fase não linear $\phi_{NLmáx} = L/L_{NL}$ (Fonte: Ref. [44])[30].

3.4.2 AOTF Não-Linear básico

Os efeitos de acoplamento e não-linearidade estão agora condensados no sistema de equações diferenciais acopladas de tal forma que:

$$\frac{dA_1}{dz} = -i\kappa_{12} A_2 - i\Delta\beta A_1 - \frac{\alpha}{2} A_1 + i\gamma |A_1|^2 A_1 \quad , \quad \text{e} \tag{3.4.5}$$

$$\frac{dA_2}{dz} = -i\kappa_{12}^{*} A_1 + i\Delta\beta A_2 - \frac{\alpha}{2} A_2 + i\gamma |A_2|^2 A_2 . \tag{3.4.6}$$

O AOTF estará operando na condição de máxima eficiência na conversão de energia entre os modos acoplados ($\kappa L = \pi/2$). Embora os pulsos emitidos por ***lasers*** possam ser

[30] Todas as figuras da seção 3.4 foram retiradas da mesma fonte.

aproximados por um perfil gaussiano, particularmente neste ponto, trabalharemos com o perfil secante hiperbólico[31]. As condições iniciais, sem ***chirp***, são dadas por:

$$A_{TE}(0,t) = \sqrt{P_0}\ \mathrm{sec}\ h\left(\frac{t}{\Delta t_0}\right)$$
$$A_{TM}(0,t) = 0 \qquad (3.4.7)$$

Para pulsos gaussianos temos que $\Delta t_1 = 2\ln(1+2^{1/2})\Delta t_0 \Rightarrow \Delta t_0 = 1{,}135$ ps. Estamos considerando $\gamma = 13\ (\mathrm{Wmm})^{-1}$.

Nas FIGURAS 3.5 e 3.6, é possível observar que a presença da não-linearidade tem forte influência na propagação do pulso. Para o primeiro comprimento $\xi_L = L/10$, o efeito na duração temporal e largura de banda do pulso não são tão significantes[32]. Entretanto, para $\xi_L = L/3$ o pulso transmitido apresenta um considerável alargamento temporal ($\Delta t = 2{,}288$ ps) e espectral ($\Delta f = 0{,}228$ THz). Para o comprimento $\xi_L = L$, o pulso chaveado apresenta uma quebra e, para comprimentos maiores, o pulso transmitido apresenta-se totalmente distorcido.

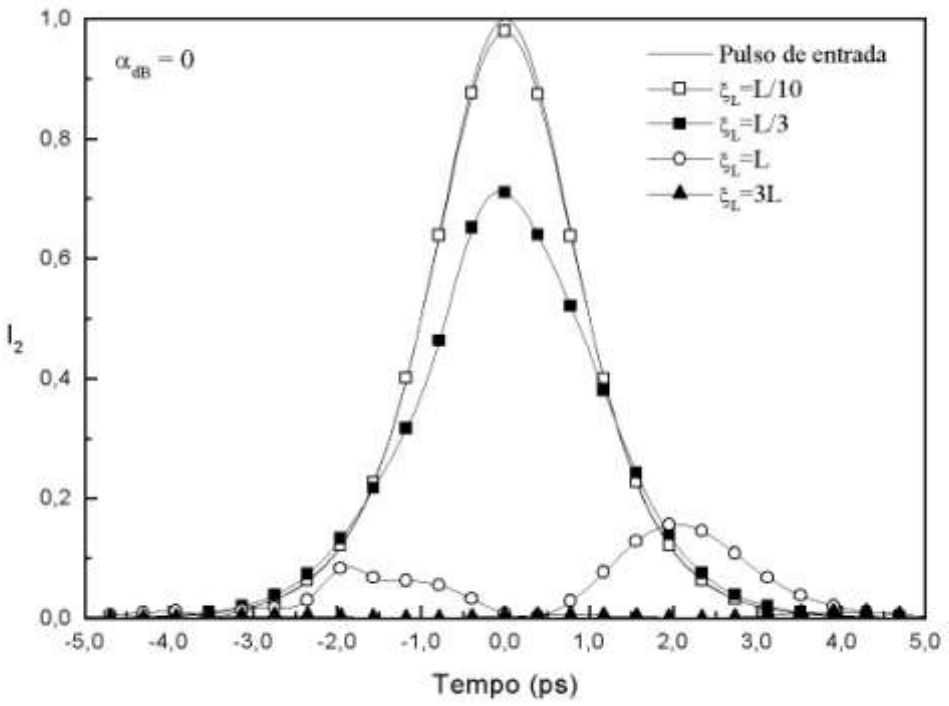


FIGURA 3.5: Intensidade do pulso de entrada no tempo e chaveado para os comprimentos $\xi_L = L/10$, $L/3$, L e $3L$ com $\kappa\xi_L = \pi/2$, $\gamma = 13\ (\mathrm{Wmm})^{-1}$ e $\alpha_{dB} = 0$.

[31] O qual ocorre naturalmente na formação de solitons ópticos.
[32] Isso será muito relevante na escolha futura desse comprimento como padrão para o processo criptográfico.

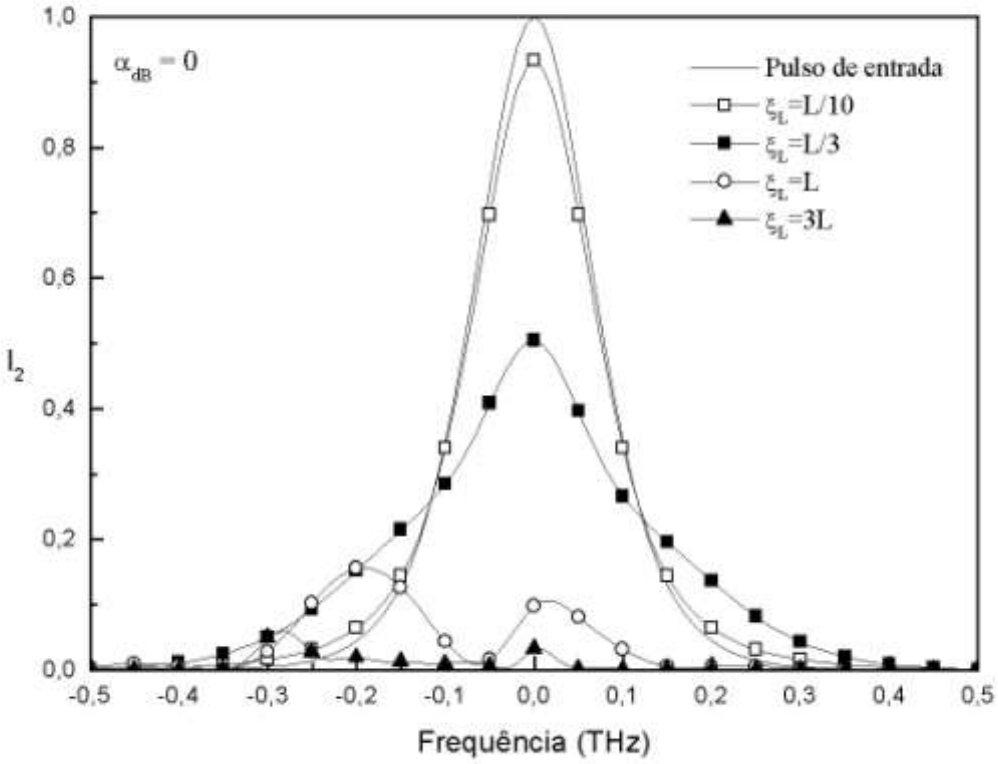


FIGURA 3.6: Intensidade do pulso de entrada na freqüência e chaveado para os comprimentos $\xi_L = L/10, L/3, L$ e $3L$ com $\kappa\xi_L = \pi/2$, $\gamma = 13\ (\mathrm{Wmm})^{-1}$ e $\alpha_{dB} = 0$.

Uma vez que dispositivos sem perda são uma situação idealizada, analisaremos o dispositivo considerando α_{dB} = 4 dB/mm para o comprimento $\xi_L = L/3$. O dispositivo sem perda já apresentava alargamento temporal (Δt_2 = 2,288 ps) para o pulso; a presença da perda deve aumentar esse efeito. Entretanto, na FIGURA 3.7 (onde o pulso encontra-se normalizado), esse efeito não é facilmente perceptível. O acréscimo temporal é bastante pequeno (Δt = 2,307 os).

No domínio da freqüência (FIGURA 3.8), a presença da perda provoca um efeito contrário, visto que, a nova largura de banda do pulso apresenta-se mais estreita (Δf = 0,195 THz) se comparada com a situação sem perda (Δf = 0,228 THz).

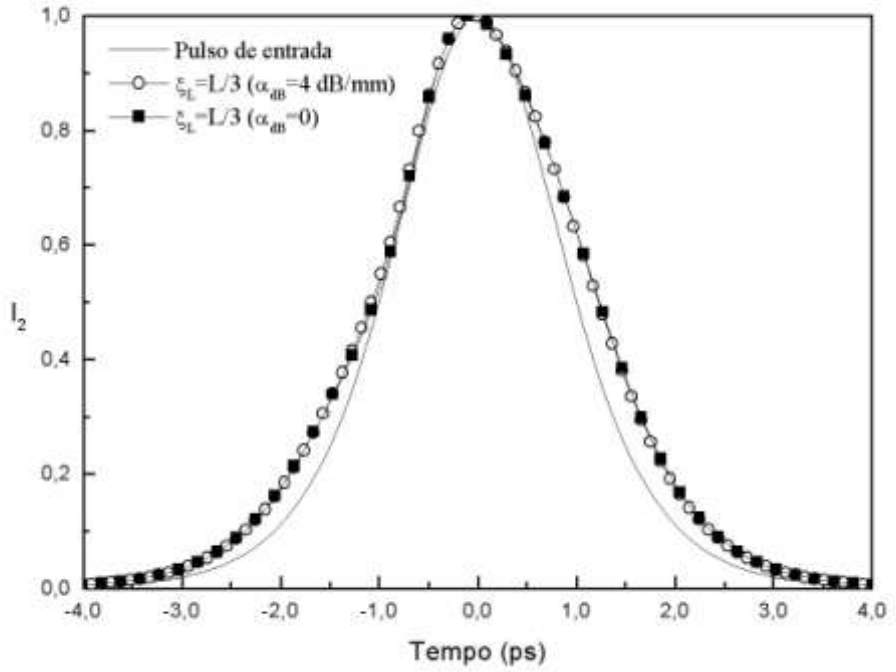


FIGURA 3.7: Intensidade do pulso de entrada no tempo e chaveado para o comprimento ξ_L = L/3, com $\kappa\xi_L$ = $\pi/2$, γ = 13 (Wmm)$^{-1}$ e α_{dB} = 0 ou α_{dB} = 4 dB/mm.

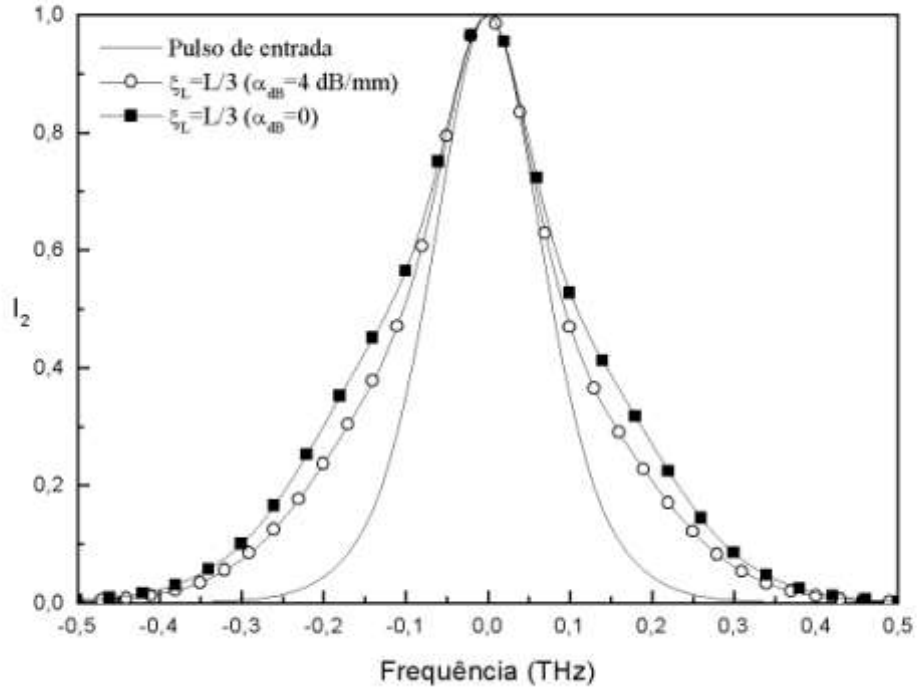


FIGURA 3.8: Intensidade do pulso de entrada na freqüência e chaveado para o comprimento $\xi_L = L/3$, com $\kappa\xi_L$ = $\pi/2$, γ = 13 (Wmm)$^{-1}$ e α_{dB} = 0 ou α_{dB} = 4 dB/mm.

3.4.3 AOTF com não linearidade crescente

Na prática as perdas assumem um papel importante, especialmente quando os materiais envolvidos na fabricação do guia de onda são semicondutores. Desta forma, quando o AOTF torna-se parte de um sistema de comunicações ópticas, podem surgir várias conseqüências decorrentes destas variações. De uma forma geral, a degradação das características originais do pulso de entrada, poderia impor limitações ou mesmo baixar o desempenho do sistema como um todo. Assim, o desenvolvimento de técnicas que possam de alguma forma manter ou recuperar o perfil do pulso propagado no AOTF, é seguramente válido.

Uma delas consiste em usar modelos predefinidos de não linearidade crescente, utilizados na confecção do guia de onda ou substrato do AOTF, com o intuito de compensar qualquer aumento na duração temporal do pulso de saída associado ao AOTF com perdas [7,47]. O modelo do AOTF com não linearidade crescente[33] e perdas pode ser derivado das equações a seguir:

$$\frac{dA_1}{dz} = -i\kappa_{12} A_2 - i\Delta\beta A_1 - \frac{\alpha}{2} A_1 + iQ(z)\gamma |A_1|^2 A_1 \qquad (3.4.8)$$

$$\frac{dA_2}{dz} = -i\kappa_{12}^{*} A_1 + i\Delta\beta A_2 - \frac{\alpha}{2} A_2 + iQ(z)\gamma |A_2|^2 A_2 . \qquad (3.4.9)$$

A FIGURA 3.9 mostra o resultado de estudos para o efeito da não-linearidade crescente com relação ao comprimento do dispositivo, relacionados com diferentes perfis[34] de não linearidade que a função $Q(z)$ poderia adotar [7,44]. Note que o valor de $Q(z)$ cresce de 1 até ρ (representando o valor utilizado anteriormente, γ = 13 (Wmm)$^{-1}$) e que ξ_L é o cumprimento do AOTF.

---

[33] Uma discussão física de como a não-linearidade crescente pode ser introduzida no material pode ser encontrada em [7,44]

[34] Constante: $Q(z) = \rho$; logarítmo: $Q(z) = \ln\{e + [(e^{\rho} - e)z]/\xi_L\}$; linear: $Q(z) = 1 + (\rho - 1)z/\xi_L$; exponencial: $Q(z) = \exp[z \ln(\rho)/\xi_L]$; gaussiano: $Q(z) = \exp\left[z^2 \ln(\rho)/\xi_L^2\right]$.

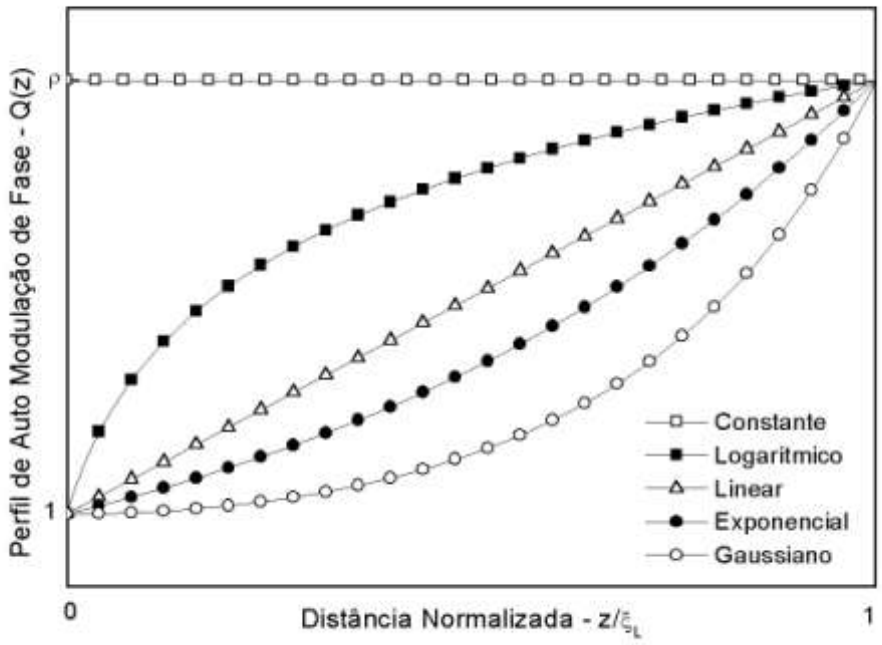


FIGURA 3.9: Curvas para diversos perfis de não linearidade utilizados na função $Q(z)$.

Para estudar as variações na duração temporal do pulso na saída ou ao longo do comprimento do AOTF, define-se o fator de compressão F_C. Ele é calculado a partir da razão entre a duração temporal do pulso chaveado Δt_2 e a duração temporal do pulso de entrada Δt_1. Naturalmente, Δt_2 será a duração temporal do pulso na saída do AOTF quando $z = \xi_L$. Assim F_C é dado por

$$F_C = \frac{\Delta t_2}{\Delta t_1}. \qquad (3.4.10)$$

O valor para F_C para a situação que tínhamos anteriormente, sem considerar os perfis de não-linearidade, é de 1,154. Na FIGURA 3.10, temos o fator de compressão para o pulso na saída do AOTF ($z = \xi_L$), em função de uma variação no valor final ρ para cada um dos perfis de não linearidade. Os valores em que $F_C < 1$ implicam em um pulso de saída com duração temporal menor do que a do pulso de entrada. Valores em que $F_C > 1$ correspondem a um pulso de saída com duração temporal maior.

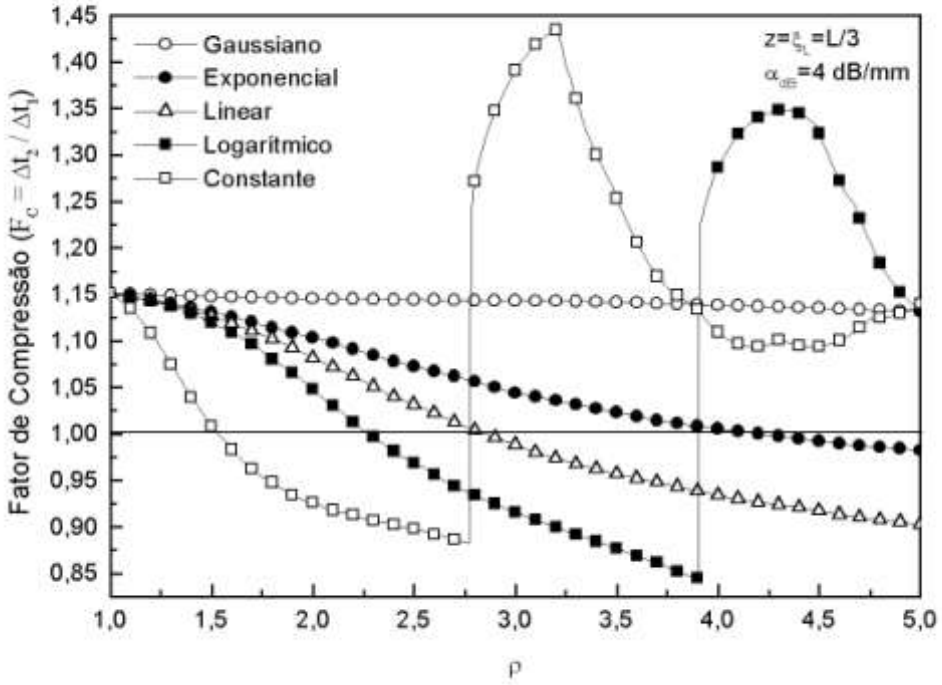


FIGURA 3.10: Fator de compressão, em função do valor final ρ, para o pulso na saída do AOTF. Os valores onde $F_C < 1$ implicam em compressão ($\Delta t_2 < \Delta t_1$) e $F_C > 1$ alargamento ($\Delta t_2 > \Delta t_1$) do pulso chaveado. As regiões de descontinuidades são indícios de que o pulso de saída apresenta quebra.

A figura nos mostra que há um valor ótimo de ρ para cada perfil considerado, onde o pulso de saída apresenta a mesma duração temporal do pulso de entrada ($F_C = 1$). Pode-se observar então que o perfil constante apresenta o menor valor ótimo (ρ_o) se comparado com os outros perfis[35]. A tabela a seguir traz um resumo para os valores ótimos de cada perfil.

TABELA 3.1: Valores finais ótimos para cada perfil e a correspondente largura temporal e espectral para o pulso chaveado (TM) na saída do AOTF. Sem perfil tem-se Δt_2 = 2,307 ps (Δf_2 = 0,195 THz) e F_C = 1,154 (Fonte: Ref. [44]).

Perfil	Constante	Logarítmico	Linear	Exponencial	Gaussiano
ρ_o	1,530	2,270	2,850	4,200	5,000
Δt_2	2,003 ps.	2,002 ps.	2,000 ps.	2,000 ps.	2,270 ps.
Δf_2	0,460 THz.	0,505 THz.	0,527 THz.	0,576 THz.	0,550 THz.

As FIGURAS 3.11 e 3.12 mostram o perfil no tempo e na freqüência do pulso de entrada e saída do dispositivo para quatro diferentes valores do parâmetro ρ (ρ = 1; 2; 2,85 e 4).

[35] As regiões onde o fator de compressão apresenta fortes descontinuidades evidenciam uma quebra no pulso de saída.

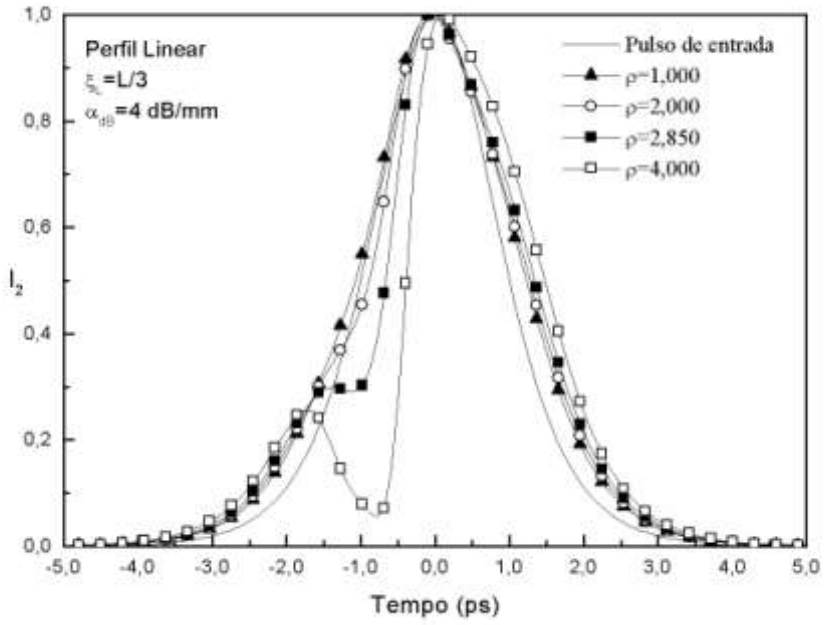


FIGURA 3.11: Intensidade do pulso de entrada no tempo e chaveado para o comprimento $\xi_L = L/3$ com $\kappa\xi_L = \pi/2$, $\gamma = 13$ (Wmm)$^{-1}$, $\alpha_{dB} = 4$ dB/mm e $Q(z)$ dado pela equação do perfil linear para $\rho = 1$; 2; 2,85 e 4.

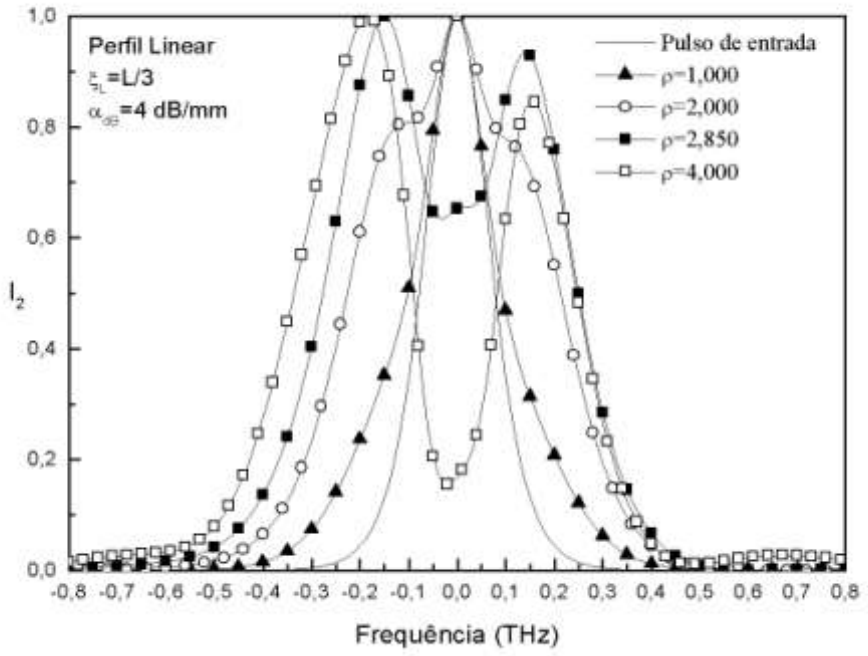


FIGURA 3.12: Intensidade do pulso de entrada na freqüência e chaveado para o comprimento $\xi_L = L/3$ com $\kappa\xi_L = \pi/2$, $\gamma = 13$ (Wmm)$^{-1}$, $\alpha_{dB} = 4$ dB/mm e $Q(z)$ dado pela equação do perfil linear para $\rho = 1$; 2; 2,85 e 4.

Observe que $\rho = 1$, na FIGURA 3.11, corresponde à situação sem a atenuação do perfil. Nesta situação, o pulso chaveado apresenta-se mais alargado ($\Delta t_2 = 2{,}307$ ps e $F_C =$

1,154), como já foi descrito antes. Em ρ = 2, o pulso ainda apresenta um perfil estável e uma duração temporal menor (Δt_2 = 2,180 ps e F_C = 1,091) do que a situação com perda e sem o perfil. Em $\rho = \rho_0$ = 2,85, devido ao aumento da não linearidade do meio, o pulso de saída está na iminência de quebrar e já apresenta uma forte assimetria temporal. Neste valor tem-se (Δt_2 = 2 ps e F_C = 1). Com o acréscimo no parâmetro ρ, há o surgimento de um ponto de quebra que divide o pulso de saída em duas partes. A parte mais intensa é mais estreita do que o pulso de entrada. Observando a Figura 3.12, nota-se que o espectro do pulso chaveado torna-se mais largo com o aumento do parâmetro ρ, e começa a desenvolver certa assimetria em ρ = 2. Igualmente ao domínio do tempo, para altos valores de não linearidade, existe a quebra ou divisão do pulso de saída [48].

3.5 Biestabilidade Óptica no AOTF

Outro fenômeno interessante que pode ser visto no AOTF é o da biestabilidade óptica. Um dispositivo biestável é aquele que possui capacidade de gerar duas saídas diferentes para uma dada entrada. Todo dispositivo desse tipo possui a combinação de um componente não-linear e alguma forma de realimentação (***feedback***) [49-52]. Desde sua descoberta, nos últimos anos de 1970, a biestabilidade óptica tem sido detectada em diferentes sistemas ópticos e um dos mais simples exemplos são os interferômetros Fabry-Perot [53]. Dispositivos biestáveis possuem diversos tipos de aplicações como, por exemplo, elementos para memória óptica, portas lógicas, chaveamento óptico, processamento de sinais, laser pulsados, etc.

Usamos pulsos ultracurtos em um AOTF, introduzindo um circuito de realimentação. Este circuito permite que uma tensão elétrica aplicada ao transdutor (SAW) mude uma das potências de saída AOTF resultando em uma resposta biestável. Pode-se mostrar as curvas de biestabilidade em função de certos parâmetros do AOTF como o produto da constante de acoplamento (κ) pelo comprimento do dispositivo (ξ_L), ou o fator de converção potência-constante de propagação (G).

3.5.1 Procedimento Experimental

Para a presente análise, utilizamos pulsos ultracurtos tipo soliton. Para pulsos solitons, a largura temporal máxima a meia altura é dada por $\Delta t_{PULSE}=2ln(1+\sqrt{2})\,\Delta t_0$. As equações do modo acoplado para descrever a evolução das amplitudes são as equações (3.4.5) e (3.4.6) [7,54].

$$\frac{dA_1}{dz} = -i\kappa_{12} A_2 - i\Delta\beta A_1 - \frac{\alpha}{2} A_1 + i\gamma |A_1|^2 A_1 \quad , \quad \text{e} \tag{3.5.1}$$

$$\frac{dA_2}{dz} = -i\kappa^*_{12} A_1 + i\Delta\beta A_2 - \frac{\alpha}{2} A_2 + i\gamma |A_2|^2 A_2 . \tag{3.5.2}$$

É preciso ressaltar que $\beta^{(2)}$, representando o parâmetro da dispersão da velocidade de grupo (GVD) do meio óptico, é negativo; caracterizando, portanto, o regime anômalo de propagação. Estamos ainda supondo a situação ideal para a conversão de potência entre os modos, $\kappa\xi_L = \pi/2$ (onde aqui ξ_L será o comprimento de interação do acústico-óptico), com a condição de Bragg satisfeita ($\Delta\beta=0$).

O procedimento proposto no presente estudo está de acordo com a FIGURA 3.13. A arquitetura do dispositivo precisou ser modificada para aquela apresentada na FIGURA 3.1; a diferença com relação ao modelo anterior está basicamente na estrutura criada para a realimentação. É possível observar que o modo TM está sendo utilizado como realimentação para o sistema. A voltagem no transdutor está diretamente relacionada com a intensidade de energia no modo TM. É essa estrutura que será responsável pela resposta biestável. A realimentação é configurada inserindo um fotodiodo (PD) juntamente com um amplificador operacional (A) [55,56]. A luz convertida entre os modos é detectada pelo fotodiodo, amplificada (A) e somada como sinal elétrico gerado no circuito de radiofreqüência (RF). Desta forma, a tensão elétrica alternada resultante, aplicada ao transdutor (SAW), pode ser influenciada pela potência de saída em um dos modos ópticos, modificando, de certa forma, as características de transmissão do dispositivo. A variação da voltagem no transdutor, por sua vez, modificará a onda acústica que irá se propagar no interior do cristal e conseqüentemente isso alterará a perturbação periódica do índice de refração. Essa mudança não só causará efeitos sobre a propagação do próprio modo TM como também do modo TE. Esta polarização, por sua vez, será a escolhida para estudarmos a biestabilidade.

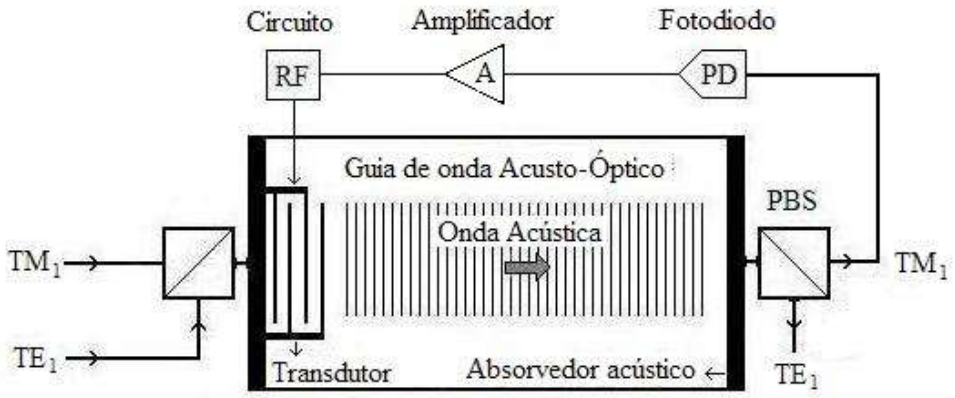


FIGURA 3.13: Modelo do filtro acústico-óptico sintonizável com estrutura de realimentação no modo TE para estudo da biestabilidade.

3.5.2 Procedimento Numérico

A forma geral para o pulso de entrada ainda será do tipo soliton e expresso matematicamente por $A(0,t) = \sqrt{P_0}\,\mathrm{sec}\,h(t/\Delta t_0)$. Inicialmente não consideraremos nenhuma potência no modo TM. A potência inicial no modo TE também irá partir de zero e aumentará gradativamente indo até um valor grande para potência uma vez que inicialmente não sabemos onde irá surgir a biestabilidade. Dessa forma a potência final escolhida é 30W. Quando variarmos a potência no modo TE, parte da energia é passada ao modo TM e isso muda a onda acústica no cristal, como discutimos anteriormente.

Para pulsos ultracurtos do tipo soliton com Δt_{pulse} = 2 ps, temos Δt_0 = 1.135ps. O comprimento do AOTF utilizado foi de aproximadamente ξ_L = 21.8 mm usando Δn = 0.07 para a birrefringência induzida no material. O coeficiente de dispersão de segunda ordem é dado por $\beta^{(2)} = -0.127\times 10^{-27}$ ps^2/mm e o de não-linearidade $\gamma = 0.098\times10^{-3}$ (W mm)$^{-1}$. Novamente, as equações acopladas (3.3.1) e (3.3.2) foram resolvidas numericamente pelo método de Runge–Kutta de quarta ordem com uma janela temporal de 1024 pontos. Consideramos a situação sem perda (α = 0). Para resolver as equações é necessário antes trocar o operador diferencial $\partial^2/\partial t^2$ por $-\omega^2$, onde ω é a freqüência no domínio de Fourier [42].

A realimentação proposta pode variar a onda acústica em sua intensidade ou em sua freqüência. Podemos considerar esses efeitos separadamente. A amplitude da radiofreqüência,

RF, controla a variação da intensidade da onda acústica e permite ajustar o nível de intensidade da luz transmitida. Isto é equivalente a variar o produto $\kappa\xi_L$ no domínio óptico. Contudo, o sinal de RF controla a freqüência da onda acústica e determina a freqüência ou o comprimento de onda da onda óptica. A variação do deslocamento de fase será analisada e interpretada a partir da seguinte expressão:

$$\Delta\beta = \Delta\beta_0 + GP_{0S} \quad . \tag{3.5.3}$$

Aqui, $\Delta\beta_0$ é o ***descasamento de fase inicial*** (sem realimentação), G entra como um fator de conversão entre a potência de conversão e a constante de propagação. Ela também permite o controle do nível da potência do modo TE, P_{0S}.

3.5.3 Resultados e Discussões

Iniciaremos a presente análise com os dados apresentados na FIGURA 3.14, logo abaixo.

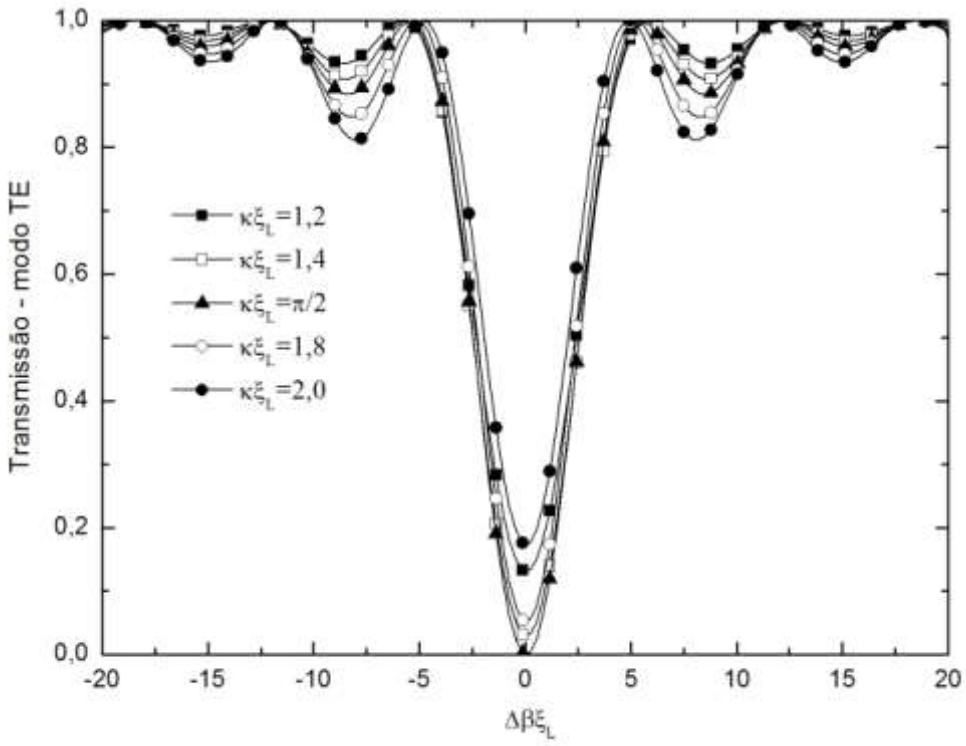


FIGURA 3.14: Curvas de transmissão para a potência de saída no modo TE.

Ela mostra que a quantidade da energia de saída contida no modo TE torna-se mínima quando o descasamento de fase tem valor próximo de zero, tornando máxima a energia de saída contida no modo TM. Além disso, ambas devem variar proporcionalmente, quando o produto $\kappa\xi_L$ assume valores diferentes. Observe que a equação (3.5.3) mostra que o descasamento de fase irá variar de acordo com o ***feedback*** introduzido no sistema. Assim, na FIGURA 3.14, o sistema proposto partirá inicialmente da situação em que $\Delta\beta\xi_L=0$, a situação de máxima transmissão, e percorrerá a curva no sentido de $\Delta\beta\xi_L$ positivo. O efeito óbvio disso é a mudança na quantidade de energia que será transmitida ao modo TM e, por sua vez, a influência na mudança na onda acústica a ser lançada no cristal. Ainda naquela, é possível perceber a diferença na transmissão quando variamos o produto $\kappa\xi_L$. A situação ideal é claramente aquela em que temos máxima transferência, ou seja, quando $\kappa\xi_L=\pi/2$. A variação nesse produto, retira o sistema dessa situação ideal e é possível ver que para quaisquer dos outros fatores escolhidos a eficiência na transferência é atenuada. Tentaremos ver então como isso afetará diretamente a biestabilidade óptica.

O fenômeno da biestabilidade óptica no AOTF pode ser comprovado a partir da FIGURA 3.15, que demonstra a obtenção da curva de histerese para os valores de $\kappa\xi_L$ = 1.2 e G = 100. O eixo das abscissas (I_i) representa a intensidade da potência de entrada no AOTF enquanto o das ordenadas (I_o) representa a intensidade da potência de saída. A trajetória indicada por ***Up*** representa o caso do aumento da potência enquanto a indicada por ***Down***, o do decréscimo.

Para condições nas quais a intensidade da potência transmitida aumenta mais rapidamente que a da incidente, a resposta não-linear do meio pode ser usada para ganho diferencial de modo similar aos transistores amplificadores. Nessa situação, uma pequena modulação da luz incidente pode ser convertida a uma grande modulação de luz transmitida. Para condições nas quais a intensidade da potência transmitida diminui mais rapidamente que a incidente, a resposta não-linear do meio pode ser usada para perda. É possível ainda podemos observar na mesma figura que a biestabilidade varia, com relação à potência de entrada, de acordo com os parâmetros escolhidos, por um intervalo de aproximadamente 20 a 22.4W. Chamaremos esse intervalo de região de biestabilidade.

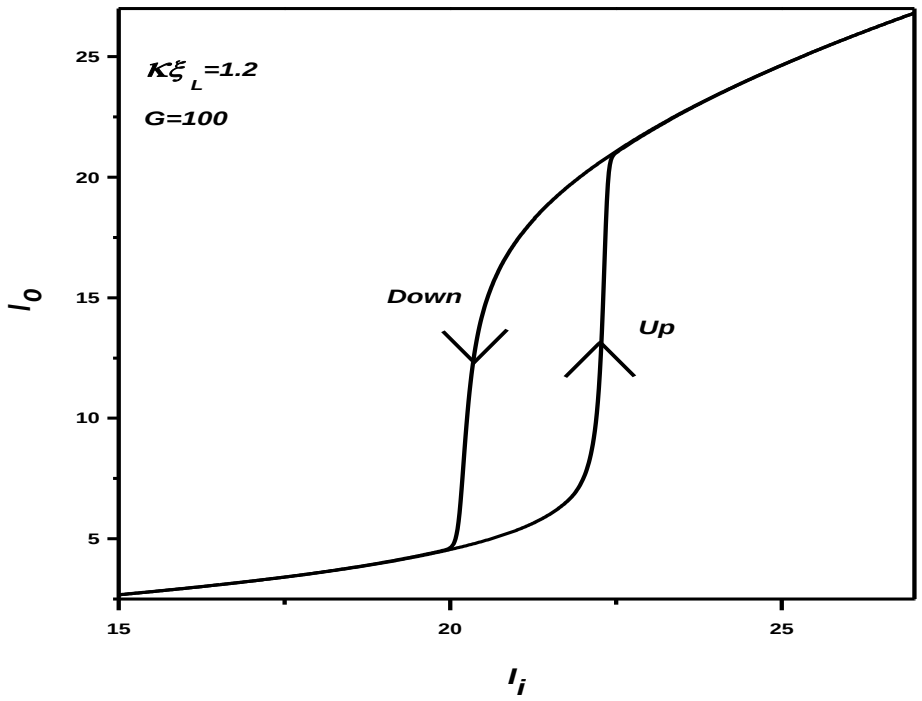


FIGURA 3.15: Curva de histerese para $\kappa\xi_L$ = 1.2 e G = 100. I_i é a intensidade da potência de entrada para o modo TE, no AOTF, e I_o é a intensidade da potência de saída.

A FIGURA 3.16, agora, fará uma análise sobre o que acontece com a região de biestabilidade quando esses parâmetros são modificados. Observamos então que ele intervalo irá variar significativamente se tanto G como $\kappa\xi_L$ mudar, como já esperávamos, pela análise que fizemos da FIGURA 3.14. Nossa abordagem se dará de duas formas: primeiro manteremos o valor de G fixo e variamos o produto $\kappa\xi_L$; a seguir manteremos esse produto fixo e variaremos o valor de G. Para as duas curvas mostradas na FIGURA 3.16, o valor do ganho foi escolhido como sendo G = 300 para ambas. Essa escolha não teve qualquer critério preferencial. Para esse valor de G, portanto, variamos o valor de $\kappa\xi_L$. O resultado é o que pode ser visto na figura.

Para $\kappa\xi_L$ = 1.2, representada pela linha sólida, o intervalo da biestabilidade óptica varia de algo em torno de 6.4 a 7.6W. Na outra curva, representando a situação cujo valor de $\kappa\xi_L$ = 1.4, essa variação é algo em torno de 6.5 a 12.2W. Quase cinco vezes maior. Uma análise mais completa do surgimento de tais intervalos distintos é possível recorrendo mais

uma vez à FIGURA 3.14. Deve-se notar que, mesmo com a variação de $\Delta\beta\xi_L$, $\kappa\xi_L$=1.2 está sempre transmitindo mais energia para o modo TM que $\kappa\xi_L$=1.4.

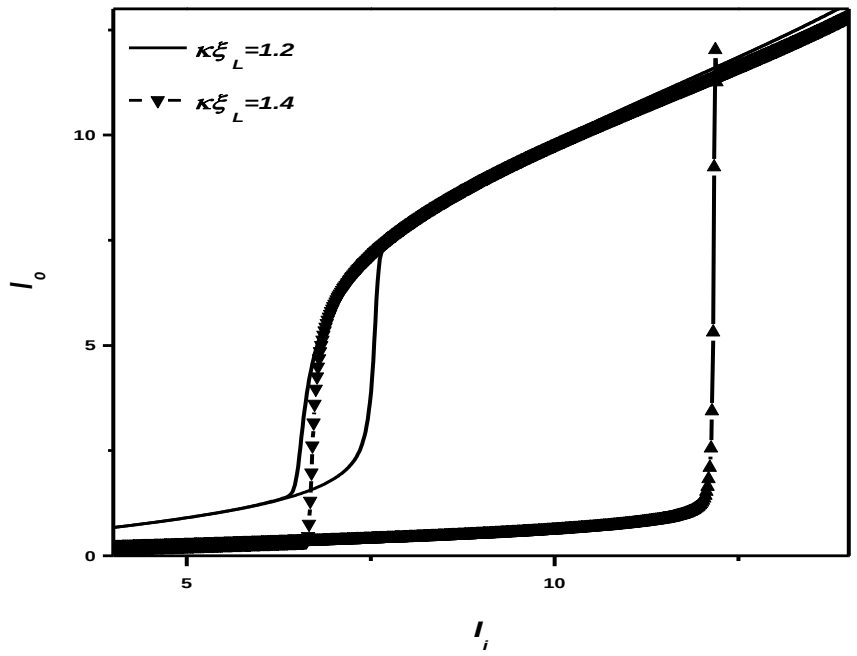


FIGURA 3.16: Curvas de histereses para G = 300 comparando as regiões de biestabilidade para $\kappa\xi_L$ = 1.2 e $\kappa\xi_L$ = 1.4.

A FIGURA 3.17, por sua vez, mostra o comportamento da biestabilidade quando o valor de $\kappa\xi_L$ é mantido fixo e G varia. Escolhemos para essa analise $\kappa\xi_L$ = 1.2 e os valores de G são indicados na figura.

A primeira coisa que se pode notar nessa figura é que com o aumento de G potencia crítica de subida tende a ocorrer para valores cada vez menores. Podemos notar também que as diferenças de intensidade entre os pulsos de saída se tornam cada vez menores. É curioso notar que os intervalos da biestabilidade não variam muito com a variação de G. Não há um comparativo na literatura para isso. Comparando estas duas ultimas figuras entre si, podemos concluir que o produto $\kappa\xi_L$ tem influência maior no valor final do intervalo de potência que delimita a faixa de biestabilidade.

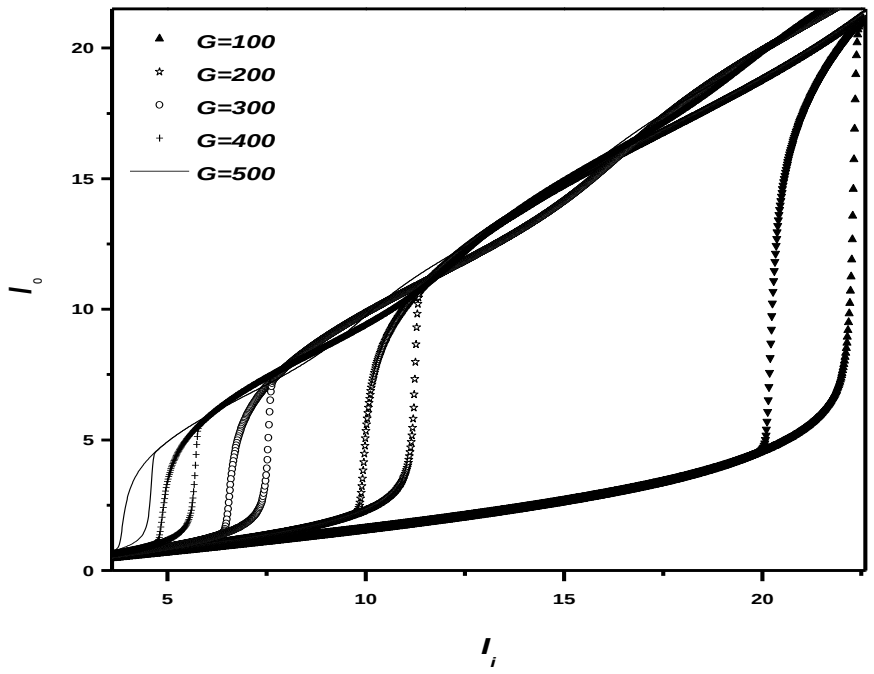


FIGURA 3.17: Curvas de histereses para $\kappa\xi_L$ = 1.2 e G variando.

3.5 Conclusões

A teoria da interação acústico-óptica nos possibilita construir dispositivos que utilizem esse efeito para selecionar as freqüências que se deseja permitir passar ou não por ele: são os filtros acústico-ópticos sintonizáveis. Realizamos um estudo analítico e numérico sobre esse dispositivo no presente capítulo. Após a descrição do esquema geral do AOTF, apresentaram-se inicialmente as curvas de transmissão para os modos eletromagnéticos TE e TM, onde podemos comprovar que a melhor transmissão ocorre quando $\Delta\beta$ =0 com $\kappa\xi_L$ =π/2. Observamos que para valores diferentes desses, a transmissão cai significativamente. O efeito na freqüência é o acentuado estreitamento de banda para valores diferentes dos citados.

Quando os efeitos de não-linearidade e perda são considerados, novos efeitos modificam ainda mais esses perfis. Estudamos vários modelos de não-linearidade e os efeitos de cada modelo estudado puderam ser vistos com detalhes. A não-linearidade Kerr dá origem a diferentes efeitos, dependendo das condições com que o sinal óptico é bombeado no guia. Dentre eles estão a automodulação de fase (SPM), a modulação cruzada de fase (XPM), a

instabilidade modulacional e outros processos paramétricos tais como geração de harmônicos, amplificação paramétrica e mistura de quatro ondas. Esses efeitos são de suma importância uma vez que são usados nas mais diversas aplicações, como chaveamento óptico, portas lógicas, compressão de pulsos, computação óptica, etc.

O termo SPM refere-se a uma mudança de fase auto-induzida, $\phi_{NL}(z,t)$, experimentada por um pulso óptico durante sua propagação em um meio dielétrico.Na prática, o termo ϕ_{NL} causa um ***chirp*** não-linear no campo transmitido. Na ausência da dispersão de velocidade de grupo (GVD), a presença de um ***chirp*** não-linear causa o alargamento espectral (em freqüência) do sinal. Este alargamento espectral é uma conseqüência da dependência temporal de ϕ_{NL} e depende do perfil do pulso considerado. O ***chirp*** não-linear, induzido pela SPM, cresce em magnitude com a distância propagada *z*, ou seja, novas componentes de freqüência são continuamente geradas à medida que o pulso se propaga no meio.

Estudos mais aprofundados foram realizados levando-se em conta perfis de não-linearidade crescente. Reproduzimos resultados já conhecidos na literatura onde se avaliou a duração temporal do pulso chaveado pelo AOTF, tomando com base para tal estudo um fator de compressão F_C. Na faixa estudada para os valores finais ρ, os perfis Constante, Logarítmico, Linear e Exponencial demonstraram possuir um valor final ótimo ρ_o, onde o pulso de saída apresentava a mesma duração temporal do pulso de entrada (F_C = 1), compensando o alargamento temporal total causado pela perda e pelo dispositivo. Mesmo considerando os valores finais ótimos ρ_o em seus correspondentes perfis, na saída do dispositivo, o pulso propagado ao longo de seu comprimento apresentou um desvios da condição desejada (F_C = 1).

Outro fenômeno interessante que pôde ser visto no AOTF foi o da biestabilidade óptica. Um dispositivo biestável é um dispositivo com capacidade para gerar duas saídas diferentes para uma dada entrada. Não nos foi possível encontrar na literatura um modelo semelhante ao proposto no presente trabalho. Usamos pulsos ultracurtos em um AOTF, introduzindo um circuito de realimentação. Este circuito permite que uma tensão elétrica aplicada ao transdutor (SAW) mude uma das potências de saída AOTF resultando em uma resposta biestável. As curvas de biestabilidade puderam ser estudadas em função de parâmetros AOTF como o produto da constante de acoplamento (κ) e o comprimento do

dispositivo (ξ_L), o fator de conversão potência-constante de propagação (G). Pudemos comprovar a forte dependência da curva de biestabilidade com relação ao produto $\kappa\xi_L$, limitando o valor final do intervalo de potência que delimita a faixa de biestabilidade.

3.6 Referências Bibliográficas

[1] GOUTZOULIZ, Akins P.; PAPE, Dennis R. (Ed.). Design and Fabrication of Acousto-optic Devices. New York: Marcel Dekker, Inc, 1994.

[2] FEICHTNER, J. D.; GOTTLIEB, M.; CONROY, J. J.. Tunable acoustooptic filters and their applications to spectroscopy. Proc. Spie 90, v. 82, p.106-118, 1976.

[3] GILLESPIE, Stacey R.; CARNAHAN, Jon W.. Ultraviolet Quartz Acousto-optic Tunable Filter Wavelength. Applied Spectroscopy, v. 55, n. 6, p.730-738, 2001.

[4] BUCHER, E. G.; CARNAHAN Jon W.. Characterization of an Acousto-optic Tunable Filter and Use in Visible Spectrophotometry. Appl. Spectrosc. n. 53, 0.603-611, 1999.

[5] BEI, Ling et al. Acousto-optic tunable filters: fundamentals: Review. Progress In Quantum Electronics, n. 28 , p.67-87, 2004.

[6] LEWIS, E. N.; TREADO, P. J.; LEVIN, I. W.. A miniaturized, no-moving-parts Raman spectrometer. Applied Spectroscopy, v. 47, n. 5, p.539-543, 1993.

[7] C.S. SOBRINHO , et al. Acousto-optic tunable filter (AOTF) with increasing non-linearity and loss. Optics Communications, v. 208, p.415-426, 2002.

[8] C.S. SOBRINHO , et al. A performance study of a logical gate using PPM optical. Optics Communications, v. 275, p.476-485, 2007.

[9] TRAN, Chieu D.. Principles and analytical applications of acousto-optic tunable filters: an overview. Talanta, Usa, v. 45, n. 2, p.237-248, 19 dez. 1997.

[10] NOBUO, Goto; YASUMITSU, Miyazaki. Wavelength-Division-Multiplex Photonic Routers with Collinear Acoustooptic Processing for Optical Label Matching in Spectral and Time Domains. Jpn J Appl Phys, Japan, v. 45, n. 5, p.4625-4630, 2006.

[11] MOLCHANOV, V. Ya. et al. An Acousto-Optical Imaging Spectrophotometer for Astrophysical. Astronomy Letters, v. 28, n. 10, p.713-72-, 28 maio 2002.

[12] KORPEL, A.. Acousto-optics. Moscou: Mir, 1993.

[13] XU, J.; STROUD, R.. Acousto-optics Devices. New York: Wiley, 1992.

[14] CHANG, I. C.. Tunable acoustooptic filtering: an overview. Proc. Spie 90, p.12-22, 1976.

[15] ANCHUTKIN, V. S.; GOTTLIEB, M.; CONROY, J. J.. Acoustooptical method of spectral–polarization image analysis. Journal Of Optical Technology, v. 76, n. , p.29-35, 1976.

[16] GUPTA, N.; VOLOSHINO, Vand B.. Development and characterization of two-transducer imaging acousto-optic tunable filters with extended tuning range. Appl. Opt. n. 46, p.1081-1088, 2007.

[17] GOLDSTEIN, S.r. et al. The Design and Implementation of a Haigh-Fidelity Raman Imaging Microscope. Journal Of Microscopy, v. 184, p.35-45, 1996.

[18] CAMPIGLIA, A. D. et al. Phosphorescence imaging system using an acousto-optic tunable filter and a charge-coupled device. Analytica Chimica Acta: Volume 346, Issue 3, p.361-372, 21 jul. 1997.

[19] CHANOVER, Nancy J.; GLENAR, David A.; HILLMAN, John J.. Multispectral near-IR imaging of Venus nightside cloud features. Journal Of Geophysical Research-planets, v. 103, p.31335-31348, 15 set. 1998.

[20] NIELD, K. M.; BITTAR, A.; HAMLIN, J. D.. Development of an all-sky-scanning spectroradiometer with a visible diode array and a near-infrared acousto-optic tunable filter. Appl. Opt., n. 36, p.7939-7947, 1997.

[21] JACKEL, J. L. et al. Acousto Optic Tunable Filters (AOTF's) for multiwavelength optical cross conects: Crosstalk Considerations. J. Lightwave Technol., n. 14, p.1056-1066, 1996.

[22] BRILLOUIN, Léon. Diffusion of Light and X-rays by a Transparent Homogeneous Body. Ann. Phys.**,** Paris, v. 17, p.88-122, 1922.

[23] DEBYE, P.; SEARS, F.w.. On the scattering of light by supersonic waves. Proc. Nat. Acad. Sci., Usa, n. 18, p.409-414, 1932.

[24] LUCAS, P.M.R., BIQUARD, P.. Le Journal de Physique et le Radium, v. 3, p. 464–477, 1932.

[25] DIXON, R. W.. Acoustic Diffraction of Light in Anisotropic Media. IEEE Journal Of Quantum Electronics, v. QE-3, n. , p.85-93, 1967.

[26] HARRIS, S. E.; WALLACE, R. W.. Acousto-Optic Tunable Filter. J. Opt. Soc. Am. v. 59, p. 744-747, 1969.

[27] CHANG, I. C.. Analysis of the noncollinear acousto-optic filter. Electron. Lett., n. 11, p.617-618, 1975.

[28] SIVARAJAN, K.n.; RAMASWAMI, R.. Optical Networks**.** San Francisco: Morgan Kaufmann Pub., 1998.

[29] MAÁK, Pál et al. Optimization of transducer configuration for bulk. Optics Communications, v. 241, p.87-98, 1997.

[30] ZAITSEV, Alexei K.; KLUDZIN, Viktor V.. Subcollinear acousto-optic tunable filter based on the. Optics Communications, v. 219, p.277-283, 2003.

[31] OSTLING, Dan; HELGE, E. E.. Acousto-optic Tunable Filters in Two-Mode Fibers. Optical Fiber Technology Research-planets, v. 3, p.177-183, 1997.

[32] HARRIS, S. E.; WALLACE, R. W.. Acousto-Optic Tunable Filter. J. Opt. Soc. Am, n. 59, p.744-747, 1969.

[33] HARRIS, S. E.; NIEH, S. T. K.; WINSLOW, D. K.. Aperture-Bandwidth Characteristics of the Acousto-Optic Filter. Appl. Phys. Lett., v. 62, n. 5, p.672-676, 1971.

[34] JACKEL, J. L. et al. Acousto Optic Tunable Filters (AOTF's) for multiwavelength optical cross conects: Crosstalk Considerations. J. Lightwave Technol, n. 14, p.1056-1066, 1996.

[35] MIDWINTER, J. E.. Photonics in Switching. Academic Press, 1993. 2 v.

[36] RAMASWAMI, R.; SIVARAJAN, K. N.. Optical Networks. Morgan Kaufmann Pub, 1998.

[37] SONG, G. Hugh. Toward the Ideal Codirectional Bragg Filter with an Acousto Optic Filter Design. J. Lightwave Technol., v. 13, n. 3, p.470-480, 1995.

[38] YARIV, Amnon; YEH, Pochi. Optical Waves in Crystals. New Jersey: John Wiley & Sons, Inc, 2003. (Wiley Classics Library).

[39] MCCORMICK, Jonh M.; SALVADORI, Mário G.. Métodos numéricos em Fortran. Polígono, 1971.

[40] HAIRER, Ernst; NØRSETT, Syvert Paul; WANNER, Gerhard. Solving Ordinary Differential Equations: Stiff and differential-algebraic problems. 2. ed. Springer, 1993. 2 v.

[41] BOYCE, William E.; DIPRIMA, Richard C.. Elementary differential equations and boundary value problems. J. Wiley, 1965.

[42] AGRAVAL, Godvin P.. Nonlinear Fiber Optics. 3. ed. Rochester, New York: Academic Press, 2001.

[43] TSAREV, A.. A new type of small size acousto-optic tunable. Applied Physics B: Lasers and Optics, v. 73, p.495-498, 2001.

[44] SARAIVA SOBRINHO , Cícero. Estudo do desempenho de filtros acústico-ópticos sintonizáveis com não linearidade crescente e perdas para aplicações em redes ópticas de telecomunicações. 2002. 73 f. Dissertação (Mestrado) - Curso de Engenharia Elétrica, Departamento de Engenharia Elétrica, Universidade Estadual do Ceará, Fortaleza, 2002.

[45] SHEN, Y. R.. Principles of Nonlinear Optics. Wiley Interscience, 1984.

[46] HELLWARTH, R. W.. Third order optical susceptibilities of liquids and solids. Prog. Quantum Electron, v.5, p. 1-68, 1997.

[47] AGULLÓ-LÓPEZ, Fernando; CABRERA, José Manuel; AGULLÓ-RUEDA, Fernando. Electrooptics - Phenomena, materials and apllications. New York: Academic Press, 1994.

[48] SILVA, M. G., et al. Analysis of Ultrashort Pulse Switching in an Acoustic Optic Tunable Filter (AOTF) with Loss. Journal of Optical Communications, v. 22, p. 228-235, 2001.

[49] BANERJEE, P. P.; POON, T. C.. Principles of Applied Optics. Q: Richard D. Irwin, Inc., 1991.

[50] WINFUL, Herbert G.; MARBURGER, J. H.; GARMIRE, E.. Theory of bistability in nonlinear distributed feedback structures. Appl. Phys. Lett., Bbb, v. 35, n. 5, p.379, 1979.

[51] STOFFERL, R.; KIVSHAR, Yu. S.. Optical bistability in a nonlinear photonic crystal waveguide notch filter. In: PROCEEDINGS SYMPOSIUM IEEE/LEOS BENELUX CHAPTER, 2000, Delft, The Netehrlands.

[52] SIEGMAN, A. E.. Lasers. Califórnia: Mill Valley, 1986. (University Science).

[53] MARBURGER, J. H.; FELBER, F. S.. Theory of a lossless nonlinear Fabry-Perot interferometer. Phys. Rev. A, Aa, v. 17, p.335-342, 1978.

[54] S. SOBRINHO , C.; SOMBRA, A. S. B.. Picosecond Pulse Switching in an Acousto-Optic Tunable Filter (AOTF) with Loss. Nonlinear Optics, v. 29, n. 1, p.79-97, 2002.

[55] ARSHIA, C.. Simulations of Bistable Acousto-Optic Devices Using MATLAB. In: PROCEEDINGS OF THE 35TH SOUTHEASTERN SYMPOSIUM. IEEE System Theory, v. 16, p. 296-298, 2003.

[56] BERNABEU, E.; MEJIAS, P. M.; MARTINEZ-HERRERO, R.. Optical Bistability: Towards All - Optical Devices. Physica Scripta, v. 36, p.312-318, 1987.

4 PROCESSO CRIPTOGRÁFICO

Dentre as tecnologias de processamento completamente óptico de sinais, a codificação completamente óptica é considerada uma função-chave para o desenvolvimento de futuros sistemas de segurança de comunicação. O processamento de informações ópticas tem demonstrado grandes potenciais como uma ferramenta promissora em aplicações na segurança [1-5]. A codificação óptica ainda possui a propriedade de que uma grande quantidade de dados pode ser armazenada ou recuperada em altos níveis de velocidade. Técnicas de codificação incluem o uso de fases randômicas [6], técnicas de polarização sensitiva [7], e diferentes tipos de técnicas digitais [8].

As características do AOTF, no que concerne aos efeitos que o pulso sofre ao passar por ele e apresentadas no capítulo anterior, nos levou a pensar na possibilidade de utilizá-lo, em acordo com algum tipo de modulação, para criptografar de alguma forma uma mensagem contida numa seqüencia de pulsos. Tal dispositivo proporcionaria um método criptográfico completamente óptico com alto desempenho. Não nos foi possível encontrar na literatura qualquer referência do AOTF sendo usado como equipamento em criptografia óptica na forma como apresentamos aqui. Na verdade, o próprio tema da criptografia óptica é bastante novo e tal área é sgnificativamente promissora, uma vez que vai ao encontro das nececidades modernas exigidas pelos sistemas de comunicação baseados em redes ópticas.

O AOTF tem desempenhado um importante papel no cenário da tecnologia fotônica e dispositivos completamente ópticos, surgindo portanto um grande interesse da parte de muitos pesquisadores [9-20]. Tal interesse se dá pelo fato dele ser o único filtro óptico capaz de selecionar múltiplos comprimentos de onda simultaneamente, já que um único cristal, do qual o filtro é basicamente constituído, pode acomodar facilmente múltiplas ondas acústicas de freqüências distintas [15,17]. Esta propriedade pode, por exemplo, ser usada para construir roteadores de múltiplos comprimentos de onda, muito importante em redes WDM. A dificuldade que pode surgir neste tipo de aplicação é o alto nível de ***crosstalk*** introduzido pelo dispositivo. O princípio básico de operação de um AOTF pode ainda ser usado para construir conexões cruzadas de múltiplos comprimentos de onda em redes WDM. Conexões cruzadas são muito importantes em redes de múltiplos comprimentos de onda, pois, permitem uma arquitetura de rede reconfigurável, de modo que a mesma pode se adaptar às mudanças no tráfico de informações. O AOTF é indicado para esta última aplicação, porque permite um

chaveamento simultâneo e independente de múltiplos comprimentos de onda (canais), escolhidos arbitrariamente e estreitamente espaçados, uma grande e flexível faixa de comprimentos de onda endereçados, rápida sintonia, baixas perdas ópticas e a possibilidade de integração de várias funções no mesmo substrato do cristal.

O dispositivo então proposto opera simultaneamente com modulação por amplitude (PAM) e por posição (PPM). O estudo foi realizado com solitons com largura temporal de 2ps. Se cada pulso é modulado simultaneamente com essas duas modulações, espera-se que cada pulso carregue dois **bits** de informação. Entretanto, quando utilizado o dispositivo, veremos que cada pulso portará não apenas dois, mas quatro **bits** de informação. Mostrado o princípio básico de funcionamento, analisaremos sua força perante ataques por usuários não autorizados.

4.1 Fundamentação Teórica

Faremos uso de dois tipos de modulação, como dito anteriormente. Dessa forma, aplicaremos aos pulsos um deslocamento temporal ($\pm\varepsilon_{PPM}$) e uma adição na amplitude ($\pm\varepsilon_{PAM}$) antes de se iniciar o processo de codificação. Essa, na realidade, por si só já um tipo de codificação. Aqui quatro bits, antes representados por quatro pulsos, são agora transformados em apenas dois pulsos.

Após a saída pelo dispositivo, o pulso será reclassificado ou não de acordo com a variação desses parâmetros. Isso se dá da seguinte forma. A modulação por posição consiste no deslocamento temporal, do pulso óptico, da posição de origem por uma quantidade ε_{PPM}. Para deslocamentos com incremento temporal positivo ($+\varepsilon_{PPM}$), a modulação representa o nível lógico 1, ou simplesmente bit 1, na modulação PPM. Para deslocamentos com incremeno temporal negativo ($-\varepsilon_{PPM}$), a modulação representa o nível lógico 0, ou simplesmente bit 0, na modulação PPM [21] (FIGURA 4.1).

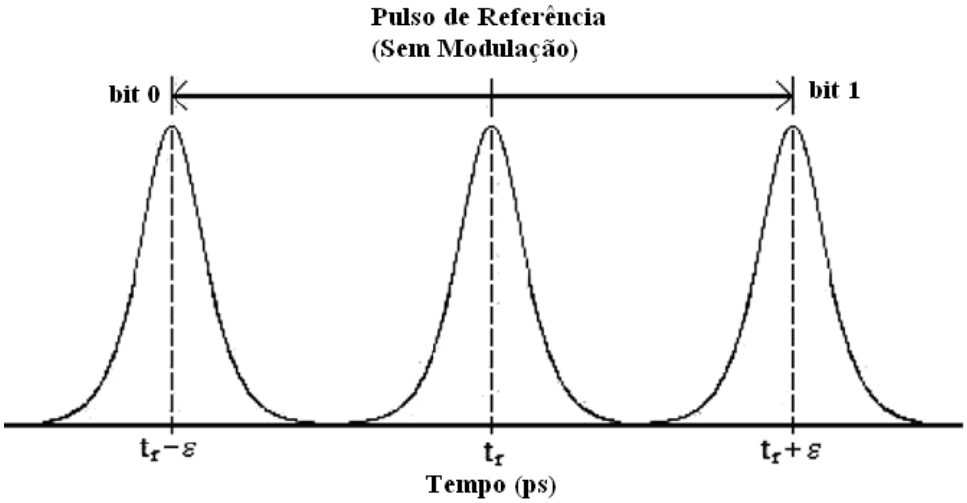


FIGURA 4.1: Modulação de pulso por posição.

Se o pulso modulado, por exemplo, no nível lógico 1, estiver fora de sua posição, durante o processo de transmissão de informação, para um deslocamento maior que o valor estabelecido ($\varepsilon > +\varepsilon_{PPM}$), então aquilo que era um bit 1 será agora interpretado como bit 0. Isso pode ser mais facilmente perceptível na FIGURA 4.2.

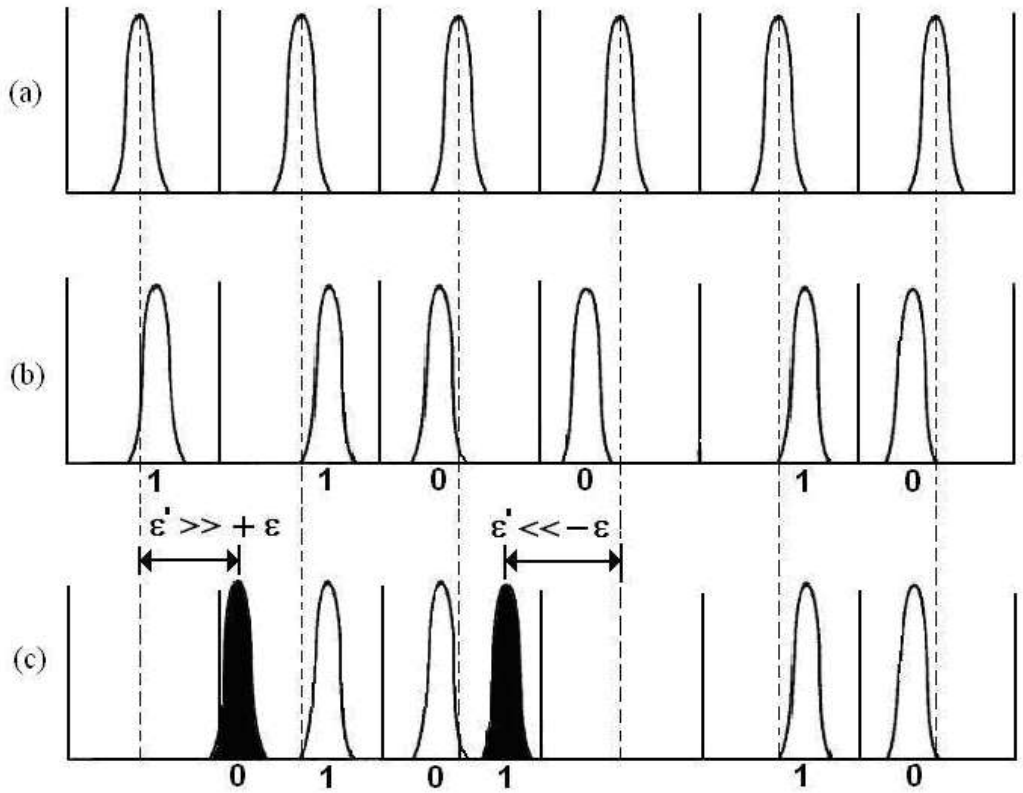


FIGURA 4.2: (a) Seqüência de pulsos não modulados por posição. (b) Seqüência de pulsos modulados por posição. (c) Indicação de erros numa seqüência de pulsos modelados por posição.

Observe que em (a) temos uma seqüência de seis pulsos sem modulação por posição. Em (b) pode-se contemplar a modulação desses pulsos pelo deslocamento temporal a partir de um tempo t_r de referência (são as linhas tracejadas em cada espaço destinado ao pulso). Já em (c), observamos o momento em que os pulsos, no decorrer de seu processo de propagação (ou qualquer outro) irá se deslocar da região em que sua modulação o estava definindo e passa a para a região de erro. Observe que o primeiro pulso, que em (b) era bit 1, avança no tempo e em (c) ele já invadiu a região de bit 0 do segundo pulso passando portanto a ser considerado bit 0 (indicado de preto em (c)). O quarto pulso, que em (b) está na região de bit 0, sofre um atraso temporal durante seu desenvolvimento e passa a ocupar a região que é de bit 1 do pulso anterior. Temos então outro erro, e o pulso que erra inicialmente bit 0, passa a ser classificado como bit 1 (também em preto em (c)). Observe ainda que nessa mesma figura, os pulsos que em (c) não aparecem em preto, não sofreram deslocamentos temporais suficientes que os retirassem de suas regiões de acerto. Ou seja, das regiões em que eles foram inicialmente modulados, suas regiões de acerto. Assim, de acordo com essa definição, a modulação do pulso por posição correspondendo ao bit 1, em todos os casos em que o deslocamento seja superior à ε_{PPM}, é considerado como erro [22]. O mesmo raciocínio é obviamente aplicado à modulação do nível lógico 0. Dessa forma, na modulação por posição, a estabilidade do pulso durante a propagação é um fator de crucial importância. Simulações computacionais demonstraram que pulsos ultracurtos possuem alta estabilidade sobre modulação PPM [22].

No caso da modulação PAM, o pulso representa o bit 1 sempre que sua intensidade for acima de um nível pré-estabelecido. As amplitudes do pulso de entrada sofrerão variação em sua amplitude de acordo com um fator $+\varepsilon_{PPM}$ e dependendo da perda ou não da amplitude no decorrer do processo, ele passa a ser bit 0 ou continua como bit 1. Como no AOTF há uma troca de energia entre os modos, adotaremos também um valor negativo para ε_{PPM}. Assim, o pulso que se inicia com um nível de energia baixo, no decorrer do processo, pode passar de bit 0 para bit1.

O processo completo do uso das duas modulações pode ser observado na FIGURA 4.3. Observe o pulso mais a direta da figura. O nível de referência para a modulação PPM é o traço pontilhado indicado pelo número 3. Qualquer pulso que se localize entre esse traço e o traço indicado pelo número 4 é considerado bit 1 na modulação PPM. Dessa forma, o pulso

que estamos analisando, por encontrar-se nessa região, é bit 1. O nível de referência para a modulação PAM é o traço indicado pelo número 1. Observe que o pulso analisado possui o seu ponto máximo de intensidade acima desse nível e é também considerado bit 1, agora na modulação PAM. Nessa mesma análise o outro pulso pode agora ser classificado como bit 0 na modulação PPM, por estar entre o traço indicado por 3 e o indicado por 2; e bit 0 na modulação PAM, por estar abaixo do traço indicado por 1.

Seria de bom alvitre criar uma nomenclatura que facilite o manuseio dessas informações. Especificaremos cada modo TE – $X_{PPM}X_{PAM}$ e TM — $X_{PPM}X_{PAM}$, onde X_{PPM}=1 ou 0 e X_{PAM}=1 ou 0, por (XXXX), onde os dois primeiros dígitos estão associados ao modo TE e os outros dois, ao TM. Assim, num exemplo em que o modo TE seja representado pelo pulso mais a direita da Figura 4.3, e o modo TM por um pulso como o mais a direita da mesma figura, teríamos TE – 11 e TM – 00. Representaríamos isso por (1100). Observe também que a modulação está associada a um par (ε_{PPM}, ε_{PAM}) que chamaremos de ***parâmetros de deslocamento***.

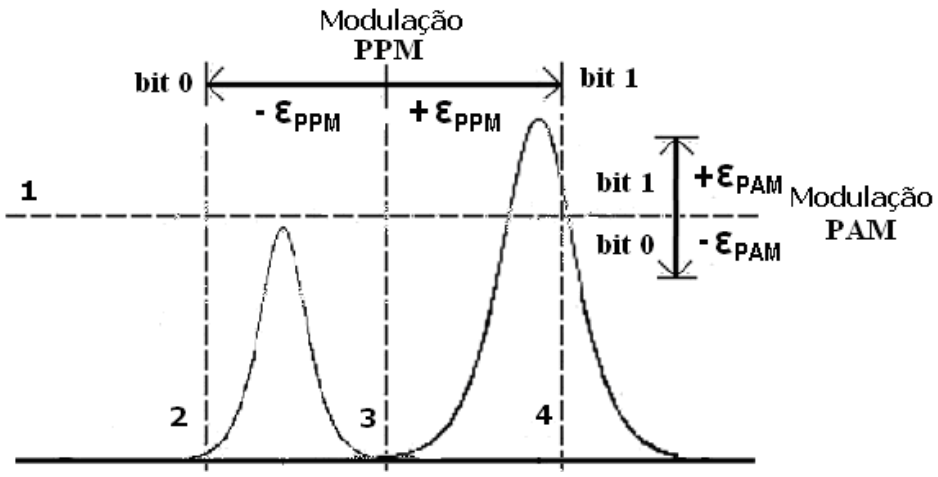


FIGURA 4.3: Simulação simultânea por posição (PPM) e por amplitude (PAM).

4.2 Procedimento Experimental

Estamos considerando os efeitos relativos dos coeficientes de dispersão $\beta^{(2)}$ e não-linearidade γ sobre pulsos propagados no AOTF. As características intrínsecas do material e do guia de onda estão relacionadas aos solitons de ordem N através da equação 4.2.1. Os pulsos de entrada (**input**) serão considerados solitons fundamentais (N=1) com

$P_0^{(N)}=(P_0^{(1)}N^2\pm\varepsilon_{PAM})$ e onde P_0 é a potencia inicial do pulso. A largura temporal máxima a meia altura é dada por $\Delta t_{PULSO}=2ln(1+\sqrt{2})\,\Delta t_0$. Uma vez que o comprimento de dispersão [$L_D=\Delta t_0^2/|\beta^{(2)}|$] está na mesma ordem de grandeza do comprimento de não-linearidade [$L_{NL}=1/\gamma P_0^{(N)}$], os efeitos dispersivos e não-lineares atuam simultaneamente na propagação do pulso. Vale ressaltar que o sinal de $\beta^{(2)}$ é negativo, uma vez que estamos no regime de propagação anômalo. Assim:

$$N^2=\frac{L_D}{L_{NL}}=\frac{\gamma P_0^{(N)}\Delta t_0^2}{|\beta^{(2)}|} \tag{4.2.1}$$

As equações diferenciais acopladas que descrevem a evolução dos modos AOTF [14,15,17] são:

$$\frac{\partial A_1}{\partial z}=-i\kappa_{12}A_2-i\frac{\Delta\beta}{2}A_1-\frac{\alpha}{2}A_1+i\gamma|A_1|^2A_1-\frac{i}{2}\beta^{(2)}\frac{\partial^2 A_1}{\partial t^2}\quad \text{TE} \tag{4.2.2}$$

$$\frac{\partial A_2}{\partial z}=-i\kappa_{12}A_1-i\frac{\Delta\beta}{2}A_2-\frac{\alpha}{2}A_2+i\gamma|A_2|^2A_2-\frac{i}{2}\beta^{(2)}\frac{\partial^2 A_2}{\partial t^2}\quad \text{TM} \tag{4.2.3}$$

onde α, κ_{12}, $\Delta\beta$, γ e $\beta^{(2)}$ ainda representam as mesmas grandezas definidas nos capítulos anteriores.

O modelo proposto para investigação do desempenho do AOTF fazendo parte de um processo de criptografia possui a arquitetura mostrada da FIGURA 4.4. Podemos inicialmente considerar uma seqüência de pulsos (1001) (podemos imaginar que esses pulsos estejam modulados tipo ***return-to-zero***[36] (RZ)) que são parte de uma longa seqüência de informação que será codificada opticamente. Em A, temos um modulador PPM/PAM. Tal seqüência chega a A onde os primeiros dois bits são polarizados no modo TM e os outros dois no modo TE. Este complexo processo, aqui representado apenas por A (e depois por C) necessita ser a uma razão de gigahertz. Um completo estudo é necessário para descrever este processo [26].

[36] A modulação ***Return-to-zero*** (RZ) descreve um código linear usado em telecomunicações no qual os sinais consecutivos retornam ao valor zero (na sua amplitude) antes de cada pulso.

No modulador proposto, o primeiro bit (no tempo) de cada par, será utilizado para definir o deslocamento na modulação PPM; o segundo para a modulação PAM. Dessa forma, o modo TE recebe (10) e o TM (01) (veja FIGURA 4.4). Os pulsos modulados são lançados no interior do primeiro AOTF e o pulso na saída do primeiro AOTF no modo TE (indicado na FIGURA 4.5 por TE') é enviado através da fibra (network). Estamos considerando aqui a situação ideal onde os pulsos não sofrem qualquer tipo de distorção através da propagação pela rede. O pulso de saída no modo TM (TM'), por sua vez, é usado para gerar a chave para a decodificação. TM' não será enviado através da fibra. A partir do par PPM/PAM escolhido, o sistema poderá ter armazenado o conjunto de chaves referentes ao par escolhido e apenas o pulso TE' será lançado. O pulso TE' é demodulado previamente em C. Neste ponto, a chave correta é identificada dentre as dezesseis possíveis chaves TM'. Quando TE' chega ao segundo AOTF, a chave TM' é lançada no modo TM. Após passar através dele, os dois pulsos de saída chegam em C onde são demodulados e a seqüência original é recuperada, caso a chave TM usada seja a correta. Ainda na FIGURA 4.4, o dispositivo B representa um polarizador. No que se encontra antes do AOTF, ele une os dois modos e naquele que se encontra depois, divide. Tanto o polarizador anterior ao AOTF quanto o posterior podem ser externos ou integrados ao dispositivo sobre o cristal. Imperfeições no polarizador (PBS) podem resultar em perdas na eficiência de chaveamento, e contribuir para algum tipo de ***crosstalk*** no AOTF.

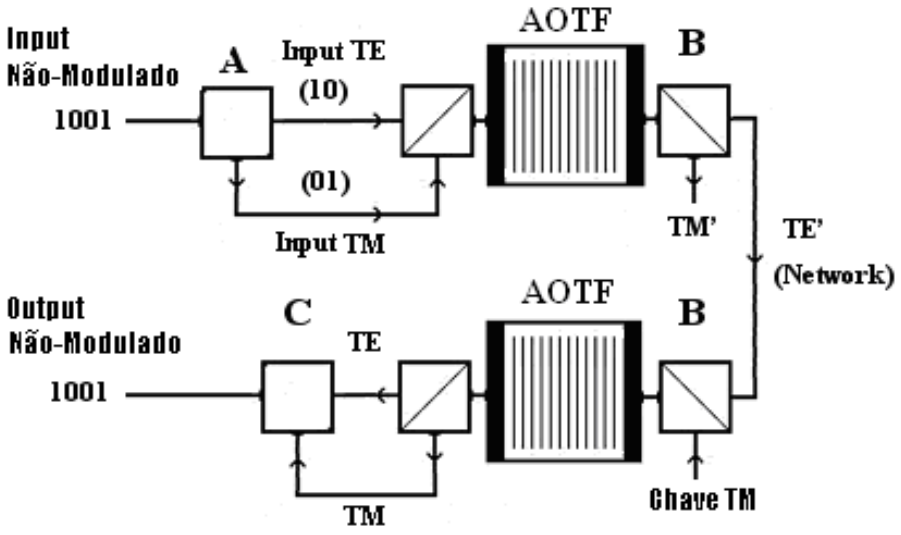


FIGURA 4.4: Processo completo de codificação. A- Modulador PAM/PPM, C- Demodulador PAM/PPM.

A informação que deve ser inicialmente transmitida de um usuário para outro é o par PPM/PAM. Com esse par, é possível gerar todas as chaves TM e recuperar a mensagem criptografada. No Capítulo 1, citamos muitas formas de trabalhar com esse problema [27]. Após a escolha do correto grupo de chaves um problema ainda permanece: como saber que chave usar para cada pulso que chega ao dispositivo. Em nossas simulações podemos perceber que cada ***input*** produzido por um par PPM/PAM é único para aquele par (obviamente podendo se repetir de alguma forma num outro par). Assim, é fácil criar uma relação entre o ***input*** no segundo AOTF e a chave correta usada para recuperar a mensagem inicial.

4.3 Procedimento Numérico

De acordo com o que foi explicado sobre a modulação simultânea sofrida por um único pulso, é possível entender que teremos, na entrada desse dispositivo, dezesseis possibilidades diferentes para a combinação entre os modos TE e TM. Por exemplo, poderemos ter (0011), (1010), e daí por diante. Dessa forma, para o estudo numérico, consideramos essas dezesseis possibilidades de combinação para os pulsos de entrada. Além disso, ainda é preciso esclarecer a análise sobre os parâmetros de deslocamento, ou seja, sobre o par (ε_{PPM}, ε_{PAM}). A variação para o parâmetro da modulação PPM será de 0 a 2ps. Em nosso modelo, essa tarefa é realizada pelo modulador PPM, antes do controle de fase. Consideramos que, no polarizador da entrada e da saída, respectivamente, as polarizações TE e TM são combinadas e divididas perfeitamente. Após passar através do primeiro polarizador, os pulsos de entrada são introduzidos no AOTF. Na região de interação, as polarizações TE e TM são convertidas, simultaneamente, como já foi amplamente discutido. No segundo polarizador, à direita, as polarizações TE e TM são divididas correspondendo ao pulso polarizado TE e ao TM na saída, respectivamente O deslocamento temporal máximo, obtido por cada pulso em suas respectivas polarizações, é calculado, considerando a sincronia com o pulso de entrada pelo tempo de referência (t_r).

Nas equações (4.2.2) e (4.2.3), o tempo $t = t' - z/\upsilon_g$ é medido do referencial que se move com o pulso na velocidade de grupo (υ_g). Analisou-se numericamente a transmissão de pulsos ultracurtos no regime de propagação de solitons de primeira ordem através das equações (4.1.2) a (4.1.3) do AOTF. Considerou-se a máxima largura temporal a meia altura igual a

Δt_{pulse} = 2 ps, correspondendo a Δf_{pulse} = 0.157 THz. Após o modulador PPM/PAM, a forma geral dos pulsos iniciais na entrada do AOTF é dada por:

$$A(0,t) = \sqrt{P_0^{(N)}}\ \mathrm{sec}\ h\left[\frac{(t - t_r - t_d)}{\Delta t_0}\right] \qquad (4.3.1)$$

onde t_d é o deslocamento temporal, que representa o parâmetro da modulação PPM (t_d=+ ε_{PPM} para o bit 1 e t_d=- ε_{PPM} para bit 0) para os pulsos de entrada. O deslocamento temporal para os pulsos de entrada e saída são calculados na posição calculada de máxima intensidade na posição temporal, com t_r = 0 como tempo de referência, correspondendo à metade da região do comprimento temporal que define a modulação (***slot***). Para pulsos ultracurtos, do tipo soliton, temos que para Δt_{pulse} = 2 ps, Δt_0 = 1.135ps. Para solitons de primeira ordem, temos N = 1 e $L_D = L_{NL}$. Além do mais, assumimos que $L_D = L_{NL}$ = L/10 (onde L aqui é o comprimento da região de interação acústico-óptica, ou seja, o tamanho do dispositivo.

Mais uma vez, para resolver o sistema de equações acopladas (aqui representadas pelas equações (4.2.2) e (4.2.3)), usamos o método de Runge-Kutta de 4ª ordem, com uma janela temporal de 1024 pontos. Mais uma vez, por questão de simplificar o problema, consideramos a situação ideal sem perda, $\alpha = 0$.

4.4 Resultados e Discussões

Nossos resultados demonstraram que a completa recuperação da mensagem inicial dependerá de algumas características que a chave correta deve ter. Estas características são o ***perfil temporal do pulso***, o ***par PPM/PAM*** usado para gerar a chave correta e a ***correspondência entre o pulso enviado e sua respectiva chave***. Inicialmente, discutiremos a primeira configuração onde temos a operação de codificação e decodificação bem sucedida. O usuário possui todas as informações corretas necessárias para recuperar a informação inicial da informação codificada. Após isso, iremos analisar inicialmente um intruso tentando recuperar a mensagem original enviada para outra pessoa usando um perfil temporal do pulso que servirá como chave. Depois, veremos o intruso usando uma chave gerada especificamente para um par PPM/PAM e tentar com ela recuperar a mensagem original criada com outro par

PPM/PAM. Finalmente, veremos o intruso tentar recuperar a mensagem original usando uma chave produzida pelo par PPM/PAM correta, mas sem a correta correspondência entre a mensagem enviada e a chave. Em outras palavras, o intruso tentaria usar a chave criada para o par (0001) para recuperar uma mensagem original (0100). Ele usa a chave gerada para a entrada (0100).

4.4.1 Correta Recuperação da Mensagem

Na FIGURA 4.2, podemos ver um exemplo da operação correta do dispositivo no que concerne ao processo de codificação/decodificação. A FIGURA 4.5(a) mostra a seqüência original antes de entrar pelo primeiro AOTF. Deve-se notar que o primeiro processo já foi realizado nesse estágio: quatro pulsos de informação foram transformados nos dois vistos na figura e tal transformação seque o processo discutido anteriormente. A seqüência original neste exemplo (1001). Ou seja, o modo TE será gerado a partir das informações dos dois primeiros bits (10) e o modo TM, dos dois últimos (01). Em cada uma dessas seqüências, o primeiro bit definirá o parâmetro para a modulação PPM e o segundo, a PAM. O resultado dessa modulação pode ser observado na figura em questão.

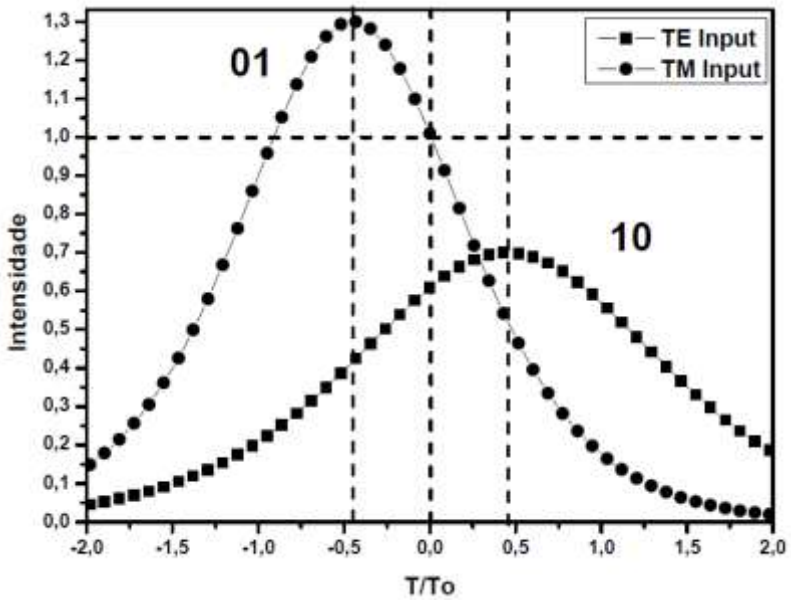


FIGURA 4.5 (a): Uso correto da chave TM e do par PPM/PAM para recuperar a informação original: seqüência inicial (1001) ainda não codificada.

Em outras palavras, pode-se notar que o pulso no modo TE encontra-se adiantado no tempo, uma vez que o bit a definir a modulação PPM é 1 e, ao mesmo tempo, encontra-se abaixo da linha de referência para a modulação PAM, cujo bit que define tal modulação é 0. Para o pulso no modo TM, há uma defasagem no tempo, uma vez que o bit para a modulação PPM é zero para este pulso e encontra-se acima da linha de referência para a modulação PAM, uma vez que o bit que a define é 1. O par PPM/PAM utilizado aqui foi (0.45;0.3).

A FIGURA 4.5(b) mostra os mesmos pulsos logo após passarem pelo primeiro AOTF, concluindo assim o processo de codificação. O pulso TE' é o pulso que será enviado pela rede contendo todas as informações dos quatro bits que formavam a seqüência inicial, a saber, (1001). TM' é a saída no modo TM. Ele é a chave gerada, mas não será lançada pela rede. É esta chave que servirá para decodificar o pulso que chega ao segundo AOTF (veja FIGURA 4.4).

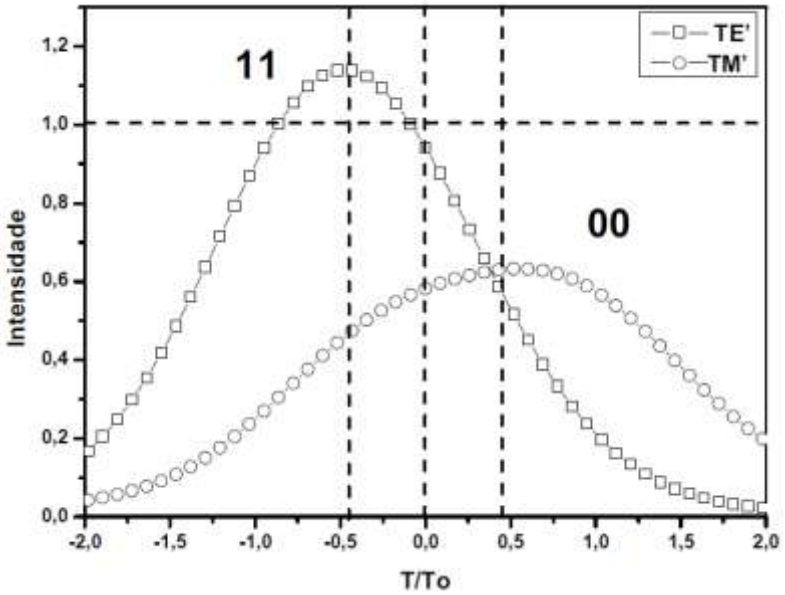


FIGURA 4.5 (b): Uso correto da chave TM e do par PPM/PAM para recuperar a informação original: pulsos codificados para a seqüência inicial (1001). TE' é enviado através da rede e a chave TM' é gerada.

No exemplo escolhido, o pulso TE' é o pulso que incidirá na entrada do segundo AOTF. Também será introduzida, nesse segundo dispositivo, a chave TM' no modo TM. Ainda neste exemplo apresentado, é possível perceber que a forma do pulso TE' é muito similar ao observado na entrada do modo TM na FIGURA 4.5(a). No entanto, indicamos o modo TM por 01, na FIGURA 4.5(a) e o modo TE (TE'), na FIGURA 4.5(b), por 11.

Observe que o pico de maior intensidade para o pulso TE’ está levemente deslocado para a esquerda da linha limite definida para a modulação PPM.

Finalmente, na FIGURA 4.5(c), temos a configuração inicial sendo reobtida. É possível perceber claramente que as intensidades dos pulsos não são as mesmas vistas na FIGURA 4.5(a). Entretanto, eles se encontram dentro das regiões das respectivas modulações onde foram inicialmente codificados.

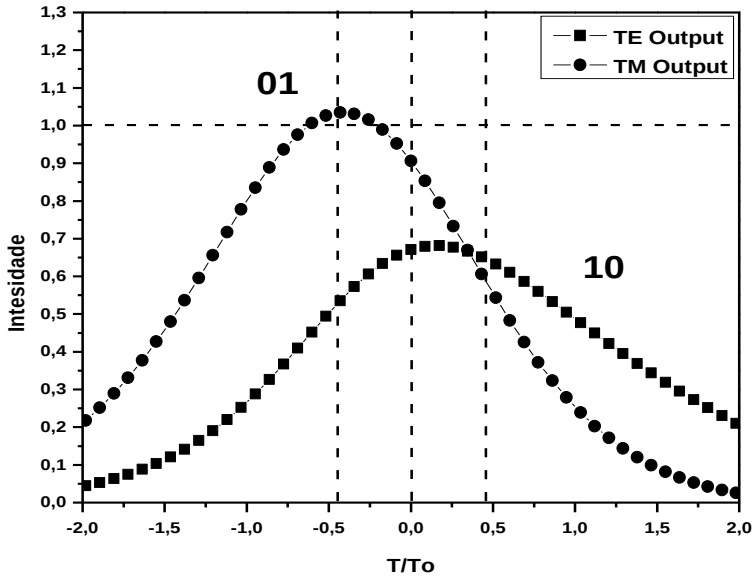


FIGURA 4.5(c): Uso correto da chave TM e do par PPM/PAM para recuperar a informação original: seqüência inicial (1001) reobitida na fase final do processo.

Com esse exemplo foi possível mostrar que a correspondência correta entre a chave TM’ e o pulso TE’ recebido, assim como do correto par PPM/PAM, possibilitam recuperar a informação codificada. É fácil ver que após passar pelo demodulador (veja FIGURA 4.4) a informação inicial, ou seja, a seqüência 1001 será corretamente restabelecida.

Tentaremos a seguir prever as possibilidades de ataque mais prováveis por um intruso que deseje interceptar uma mensagem originalmente destinada a outro usuário da rede.

4.4.2 Ataque com Perfil Temporal Tipo Soliton

O primeiro ataque sugerido ao sistema proposto trata-se de um intruso que de alguma forma conseguiu uma informação sobre a intensidade da chave e sua localização temporal,

mas não sabe a forma exata do perfil. Para piorar o quadro, vamos imaginar que esse invasor de alguma maneira obteve acesso ao correto par PPM/PAM (0.45;0.3). Na FIGURA 4.6(a) podemos visualizar a mesma situação inicial descrita na FIGURA 4.5. Estamos usando a mesma seqüência de pulsos (1001) e a figura a seguir representa os modos TE e TM após passarem pelo primeiro AOTF.

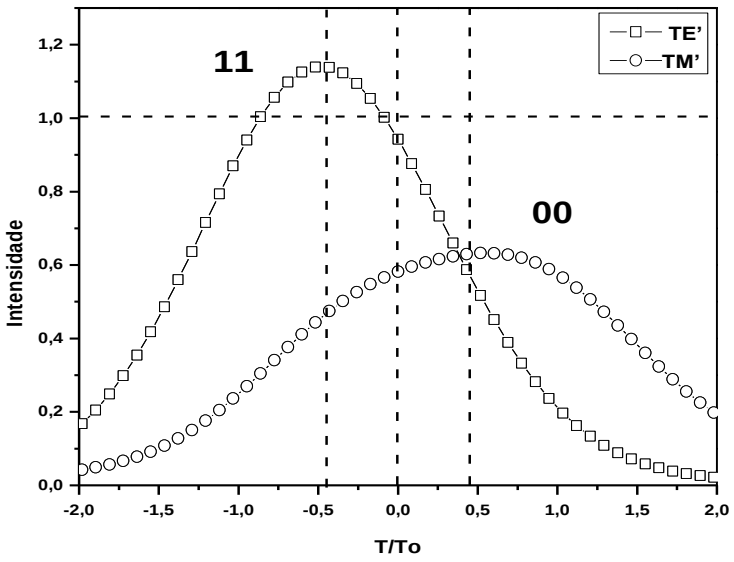


FIGURA 4.6(a): Uso de um perfil diferente para a chave TM' (perfil tipo soliton) para tentar recuperar a informação inicial (0110). TE' é o pulso codificado que é enviado pela rede e TM' é a chave usada para recuperar a seqüência original.

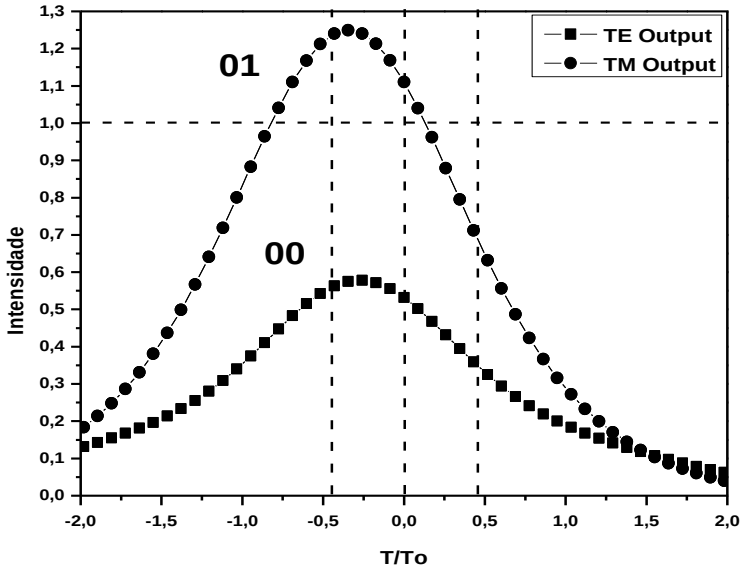


FIGURA 4.6(b): Decodificação mal sucedida para o uso de um perfil diferente para a chave TM' (perfil tipo soliton).

É difícil perceber as diferenças entre o perfil usado aqui (usou-se um perfil tipo soliton com a mesma amplitude da chave TM' correta, A=0.6) e o correto. No entanto, a FIGURA 4.6(b) mostra claramente que o perfil utilizado invalida a chance de recuperar a mensagem inicial. Vemos que a seqüência obtida foi (0001), quando deveríamos obter (1001).

4.4.3 Ataque com Relação Errada entre a Chave e o Pulso de Informação Codificado

O próximo ataque serve para demonstrar que a chave TM' só pode ser usada para decodificar o pulso TE' ao qual ela está relacionada. Vamos supor agora que o intruso conheça o perfil correto da chave TM' e ainda conheça o par PPM/PAM correto. No presente exemplo, a mensagem original é (1101). O par PPM/PAM usado para codificá-la foi (0.45;0.3). A FIGURA 4.7(a) mostra a seqüência original logo após o processo de modulação e pronta para passar pelo primeiro AOTF.

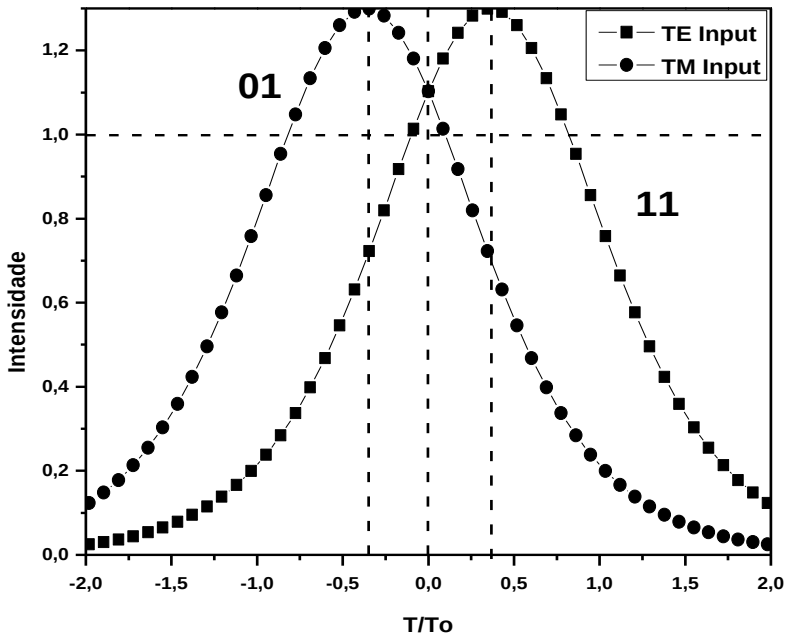


FIGURA 4.7(a): Um intruso tenta usar uma chave TM', produzida pela entrada (0110), para decodificar TE', produzida a partir da entrada (1101): seqüência original logo após o processo de modulação e pronta para passar pelo primeiro AOTF.

A FIGURA 4.7(b), por sua vez, trás o pulso TE' após passar pelo primeiro AOTF e a chave TM', gerada pela seqüência original (0110). Essa chave será usada para tentar decodificar a informação trazida por TE', originado da seqüência (1101). A FIGURA 4.7 (c) mostra que, mais uma vez, o intruso não teve sucesso em obter a mensagem original. A mensagem obtida foi (1000).

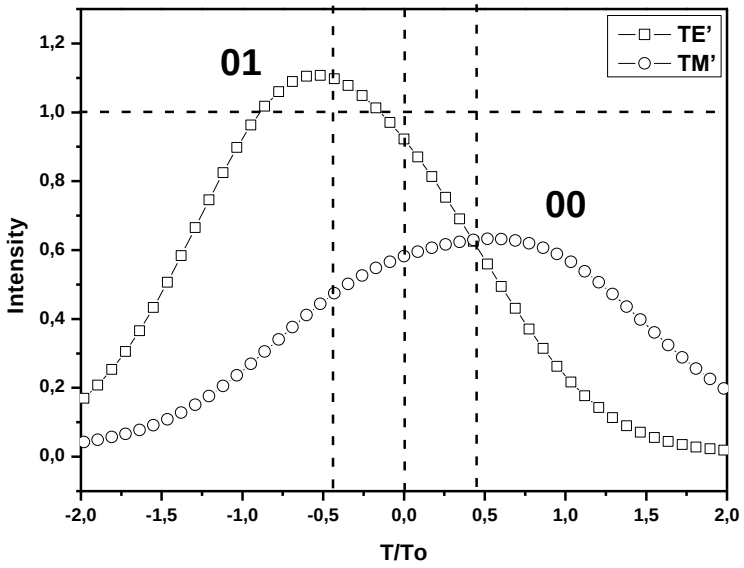


FIGURA 4.7(b): Um intruso tenta usar uma chave TM', produzida pela entrada (0110), para decodificar TE', produzida a partir da entrada (1101): TE' na entrada do segundo AOTF com a chave TM' errada.

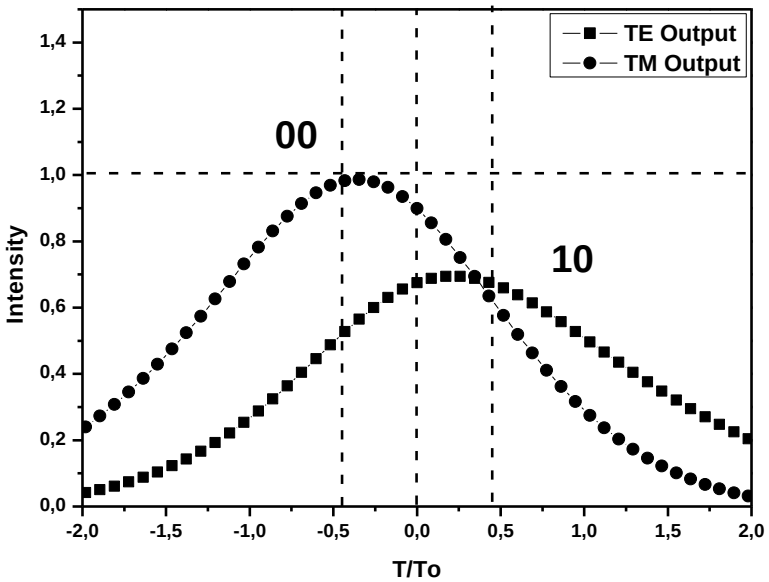


FIGURA 4.7(c): Um intruso tenta usar uma chave TM', produzida pela entrada (0110), para decodificar TE', produzida a partir da entrada (1101): seqüência logo após a passagem pelo segundo AOTF. O intruso não teve sucesso em obter a mensagem original. A mensagem obtida foi (1000) e a original (1101).

4.4.4 Ataque com o Par PPM/PAM Errado

O próximo ataque será com o uso errado do par PPM/PAM. O intruso irá utilizar o correto perfil da chave TM' assim como a correta correspondência entre a chave e o pulso TE'.

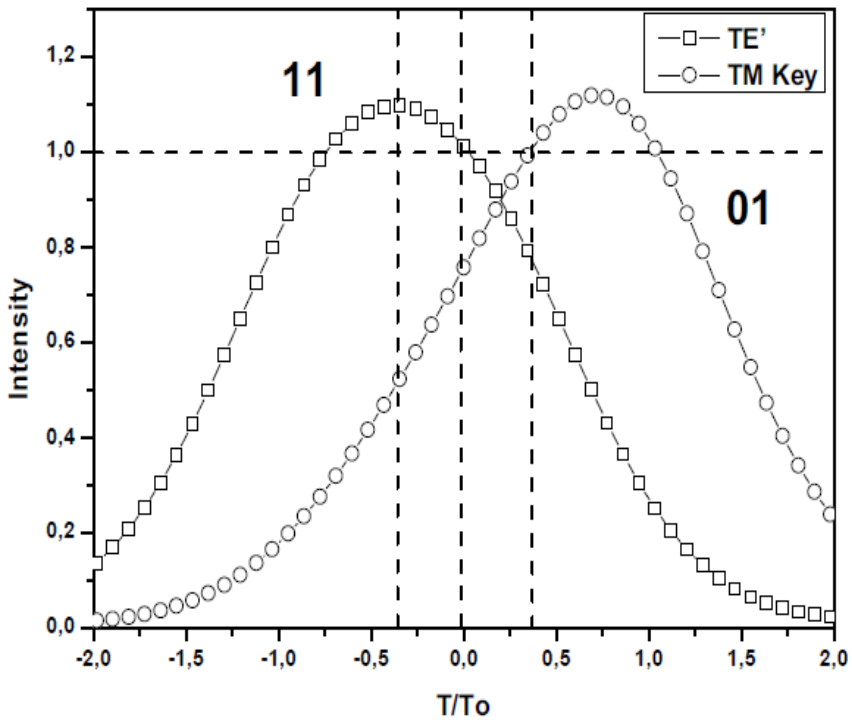


FIGURA 4.8(a): Um intruso tenta obter a informação gerada pelo par PPM/PAM (0.3; 0.45), utilizando uma chave TM', gerada pelo par PPM/PAM (0.25; 0.36): TE' na entrada do segundo AOTF com a chave TM' errada.

No exemplo escolhido, a mensagem original foi codificada usando o par PPM/PAM (0.45;0.3). A chave usada pelo intruso, entretanto, foi produzida a partir do par (0.36;0.25). A situação original é a mesma apresentada na FIGURAS 4.7(a). A FIGURAS 4.8(a) mostra o pulso TE', antes de entrar no segundo AOTF, e a chave TM' errada.

Na FIGURA 4.8 (b), vemos o resultado final na saída no segundo AOTF. É possível ver facilmente que a mensagem original não foi obtida com sucesso. A mensagem correta seria (1101) enquanto que o intruso obteve (0101). A mensagem está protegida.

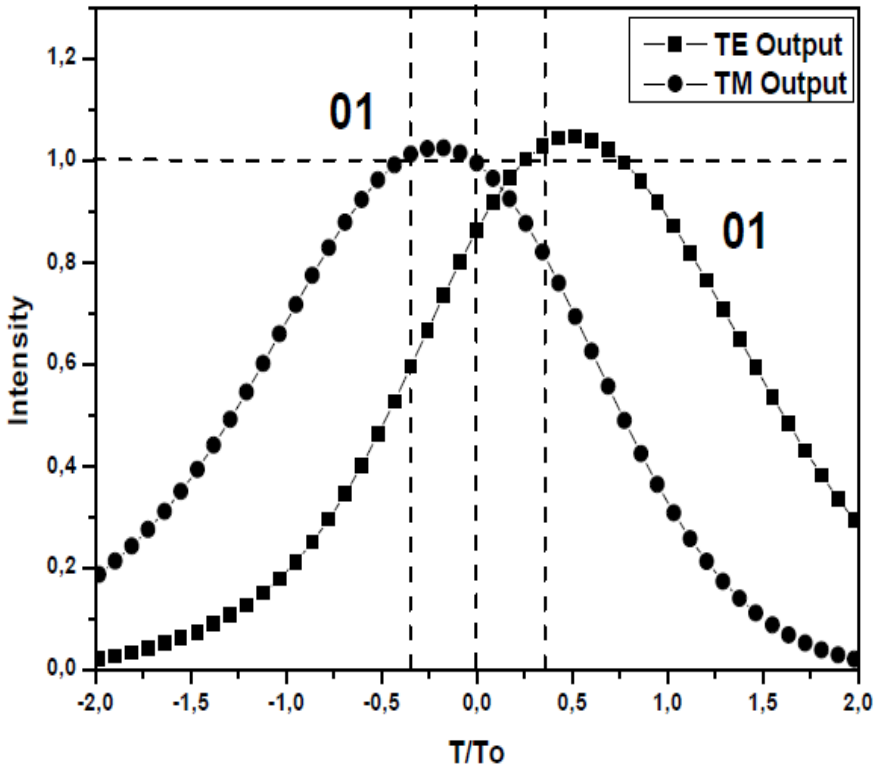


FIGURA 4.8(b): Um intruso tenta obter a informação, gerada pelo par PPM/PAM (0.3; 0.45), utilizando uma chave TM', gerada pelo par PPM/PAM (0.25; 0.36): seqüência logo após a passagem pelo segundo AOTF. O intruso não teve sucesso em obter a mensagem original. A mensagem obtida foi (1101) e a original (0110).

4.4.5 Regiões de Validade para a Codificação

Discutidas as possibilidades de ataque, torna-se necessário agora definir, para a situação ideal, descrita na secção 4.4.1, a região de validade com relação aos parâmetros do par PPM/PAM. Isso porque alguns pares PPM/PAM, mesmo utilizando todos os parâmetros de forma correta, ainda assim não servirão ao processo da criptografia aqui proposto. O motivo para isso é bastante simples.

Suponha que o valor, no par PPM/PAM, do parâmetro para a modulação PAM seja ε_{PPM}= 0.1. Como foi discutido no Capítulo 3, ao passar pelo AOTF, o pulso sofre um pequeno espalhamento no tempo, perdendo portanto um pouco de sua altura. Mesmo no AOTF sem perda esse fenômeno ainda é perceptível. Se o valor para o parâmetro para a modulação PAM for muito pequeno, como no exemplo aqui citado, o pulso perderá sua intensidade e essa perda apenas se acentuará ao passar pelo Segundo AOTF, responsável pelo processo de decodificação. O pulso sofrerá então dois decréscimos em sua intensidade e não poderá ser

lido como bit 1 na modulação PAM. Assim, apenas intensidades máximas que compensem essa perda poderão passar pelo processo criptográfico com sucesso.

Além disso, as distâncias temporais entre esses pulsos, na entrada do AOTF, ou seja, o valor do parâmetro para a modulação PPM, irão influenciar no processo de troca de energia entre os modos. Assim, para uma dada intensidade PAM ainda deve ser levada em consideração o efeito da modulação PPM, para evitar o mesmo efeito de erro que acabamos de descrever.

Destarte, a FIGURA 4.9 mostra todos os possíveis pares PPM/PAM para os quais o processo de codificação funcionará usando a mensagem original (0110). O eixo das abscissas representa o parâmetro da modulação PPM e o das ordenadas, o da modulação PAM. O parâmetro para a modulação PPM foi variado de 0.2 a 1ps; o parâmetro para a modulação PAM foi variado de 0.1 a 0.5 da amplitude limite. A região negra representa os pares permitidos, ou seja, aqueles cuja codificação irá funcionar. Tomemos, por exemplo, o par PPM/PAM (0.4;0.25). Se traçarmos uma reta, paralela ao eixo vertical, cortando o horizontal no valor 0.4 e, de forma semelhante, traçarmos uma reta, paralela ao eixo horizontal, cortando o vertical em 0.25, a interseção entre essas duas retas cairá sobre uma região negra. Assim, o par (0.4;0.25) é um par permitido.

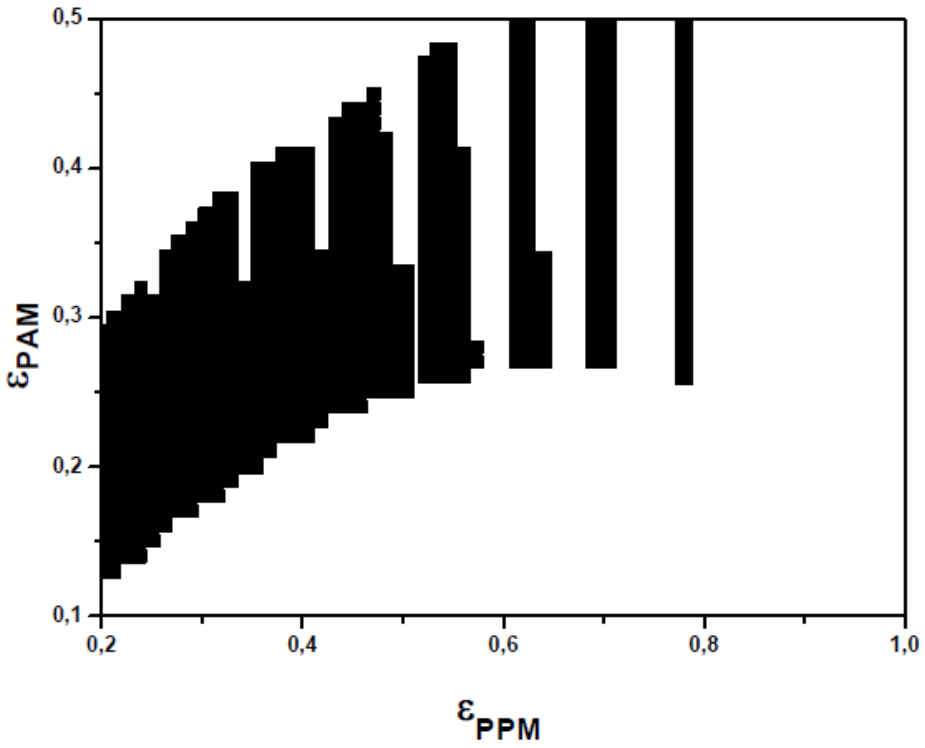


FIGURA 4.9: Região permitida para os pares PPM/PAM para a entrada (0110).

Por outro lado, se realizarmos o mesmo procedimento para o par (0.6;0.2), veremos que agora caímos numa região branca. Assim o dado par não é possível para a criptografia da entrada (0110).

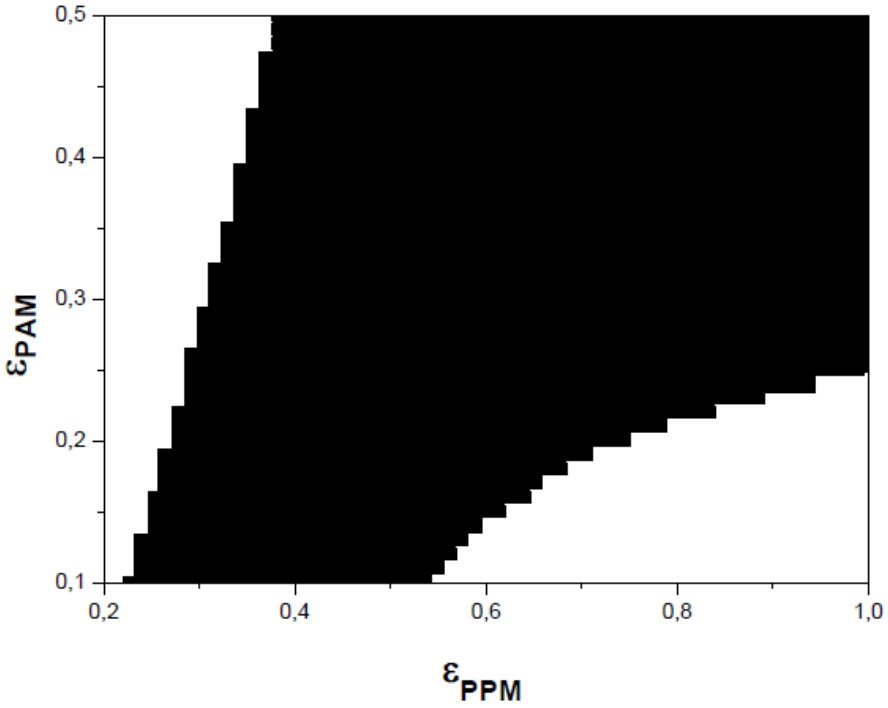


FIGURA 4.10: Região permitida para os pares PPM/PAM para a entrada (1011).

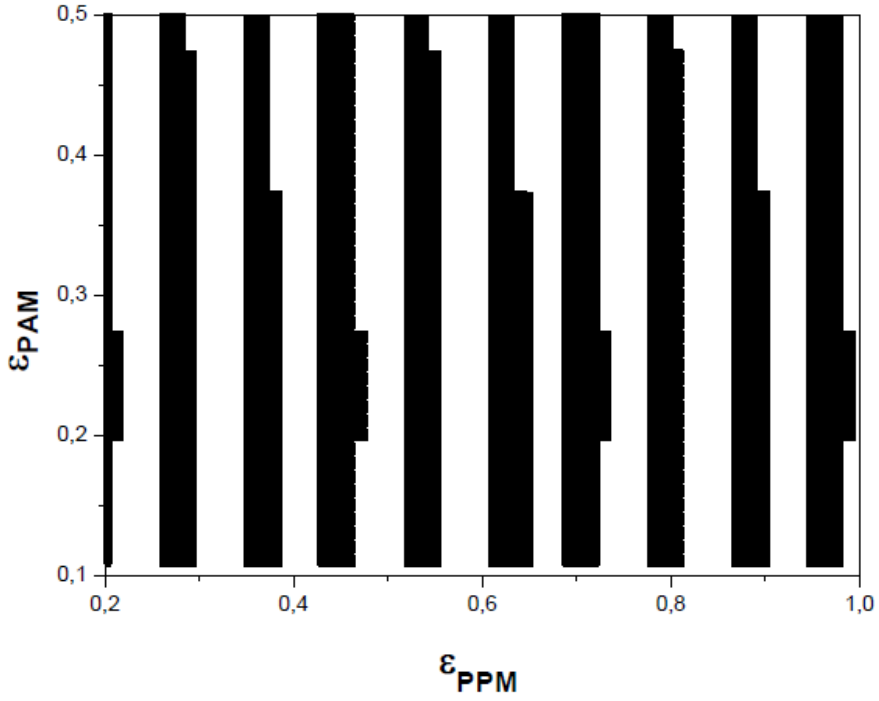


FIGURA 4.11: Região permitida para os pares PPM/PAM para a entrada (0000).

Nas FIGURAS 4.10 e 4.11, vemos as regiões de validade para mais outras duas entradas. São elas (1011) e (0000). É possível perceber claramente que essas figuras não necessitam de modo algum ser semelhantes. Na realidade, cada entrada produzirá uma figura característica. As dezesseis entradas não apareceram aqui por motivos óbvios de espaço. Mesmo porque a figura realmente significativa deve partir do seguinte princípio.

Para que o dispositivo funcione corretamente, para um dado par PPM/PAM, devemos ter uma região negra para todas as entradas. Senão vejamos. Tomemos como exemplo o par PPM/PAM (0.2;0.2) para a entrada (0110), na FIGURA 4.9. Pode-se observar que o ponto determinado por esse par cai numa região negra. Logo o processo de codificação é permitido. Por outro lado, quando tomamos o mesmo par para a entrada (1011), FIGURA 4.10, vê-se claramente que a região é clara. Logo, o processo não é permitido para tal entrada usando o par (0.2;0.2). Conclui-se com isso que este par PPM/PAM não pode ser usado para o processo de codificação, uma vez que, numa longa mensagem, será quase impossível a seqüência de bits 1011 nunca aparecer. Sempre que ela aparecer, o dispositivo irá falhar quando a mensagem precisar ser decodificada.

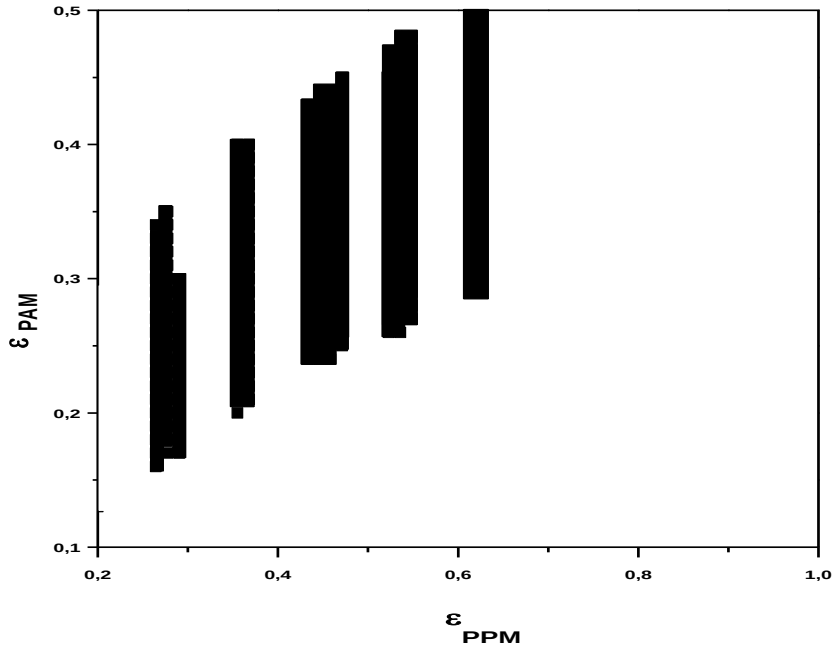


FIGURA 4.12: Superposição de todas as dezesseis regiões permitidas para os parâmetros PPM/PAM.

Com base nesse raciocínio, fica claro entender que a região em que o dispositivo funcionará corretamente, considerando essas duas entradas, será a região de intersecção das

áreas negras entre as FIGURAS 4.9 e 4.10. Podemos agora generalizar o que acabamos de dizer para todas as entradas. Ou seja, o dispositivo só irá funcionar corretamente na região de intersecção das áreas negras para todas as dezesseis possíveis entradas. O resultado disso encontra-se na FIGURA 4.12.

4.5 Conclusões

Foi possível observar que o modelo de criptografia proposto foi resistente aos sugeridos ataques de intrusos que desejavam obter informações destinadas a outros usuários da rede. Testamos a eficiência do dispositivo com relação a esses ataques e o mesmo mostrou-se seguro. Após apresentar, portanto, o funcionamento do dispositivo, foi necessário definir para quais valores de pares PPM/PAM ele realmente funcionaria. Discutiu-se que certas considerações, com relação à própria natureza do funcionamento do AOTF, iria invalidar certos grupos de chaves, de tal forma que foi preciso definir mais precisamente quais seriam.

Dessa forma, o produto cartesiano entre os conjuntos dos valores de ε_{PPM} (o intervalo contínuo que vai de 0.2 a 1) e de ε_{PAM} (o intervalo contínuo de 0.2 a 0.5) cria uma região em que é possível analisar a validade do funcionamento do dispositivo para o par PPM/PAM escolhido para cada entrada específica de um conjunto de quatro **bits**. O perfeito funcionamento do dispositivo somente é possível com a intersecção dessas regiões para os dezesseis tipos diferentes possíveis de entradas de quatro **bits**. Essa região foi então definida e nesses pontos o dispositivo funciona com sucesso. Cada ponto possível dessa região está associado com um par PPM/PAM que dois usuários podem usar para se comunicar entre si, numa rede, protegidos dos demais usuários.

4.6 Referências Bibliográficas

[1] JAVIDI, B.; HORNER, J.L.. Optical pattern recognition for validation and security verification. Opt. Eng., v. 33, n.6, p.1752-1756, 1994.

[2] JAVIDI, B.; AHOUZI, E.. Optical Security System with Fourier Plane encoding. Appl. Opt., v. 37, n. 26, p.6247-6255, 1998.

[3] MATOBA, O.; JAVIDI, B.. Encrypted Optical Storage with Angular Multiplexing. Appl. Opt., v. 38, p. 7288, 1999.

[4] TAN, X., et al. Secure Optical Storage that Uses Fully Phase Encryption. Appl. Opt., v.39, p. 6689, 2000.

[5] LAI, S.; NEIFIELD, M.. Optical encryption method using toroidal zone plates. Opt. Commun., v. 1-3, n. 248, p.35-40, 2000.

[6] RÉFRÉGIER, P.; JAVIDI, B.. Optical image encryption based on input plane and Fourier plane random encoding. Opt. Lett. n. 20, v. 17, p.767-769, 1995.

[7] ARIZAGA, R.; TORROBA, R.. Optical encryption method using toroidal zone plates. Opt. Commun. n. 248, v. 1-3, p. 35-40, 2005.

[8] BARRERA, John Fredy et al. Multiplexing encrypted data by using polarized light. Physica Scripta, v. 260, n. 1, p.109-112, 1 abr. 2006.

[9] SOBRINHO, C. S.; LIMA, J. L. S.; SOMBRA, A. S. B.. Interchannel Crosstalk on the Acousto-Optic Tunable Filter (AOTF) for Network Applications. Microwave And Optical Technology Letters, v. 35, n. 2, p.230-235, 2002.

[10] SOBRINHO, C. S., et al. Numerical Analysis of the Crosstalk on an Integrated Acousto-Optic Tunable Filter (AOTF) for Network Applications. Fiber and Integrated Optics, v. 35, n. 5, p. 345-363, 2004.

[11] ONAKA, H., et al. Compact photonic gateway for dynamic path control using acousto-optic tunable filter. Optical Switching and Networking, v. 5, p. 75-84, 2008.

[12] VEERIAH, Sutharsanan; RAHMAN, Faidz Abd; MISHRA, Vivekanand. Multiple parameter tuning of the bandwidth, wavelength and attenuation of a fiber-based acousto-optic tunable filter. Optik, n. 118, p.481-486, 2007.

[13] SOBRINHO, C. S., et al. Acousto-Optic Tunable Filter (AOTF) Revisited: Ultrashort Optical Pulses Crosstalk Studies on the Lossy Filter. Fiber and Integrated Optics, n. 25, v. 3, p. 195-211, 2006.

[14] SOBRINHO, C. S.; SOMBRA, A. S. B.. Picosecond Pulse Switching in an Acousto-Optic Tunable Filter (AOTF) with Loss. Nonlinear Optics, n. 29, v. 1, p. 79- 97, 2002.

[15] SOBRINHO, C. S., et al. Acousto-optic tunable filter (AOTF) with increasing non-linearity and loss. Optics Communications, v. 208, p.415-426, 2002.

[16] GAO, L.; HERRIOT, S. I.; WAGNER, K. H.. Novel Approach to RF Photonic Signal Processing Using an Ultrafast Laser Comb Modulated by Traveling-Wave Tunable Filters. IEEE Journal of Selected Topics In Quantum Electronics, n. 12, v. 2, p. 315-329,2006.

[17] FERREIRA, A. C., et al. A performance study of an all-optical logic gate based in PAM-ASK. Journal of Modern Optics., n. 56, v. 8, p. 1004-1013, 2009.

[18] SOBRINHO , C. S.; RIOS, C. S. N.; SOMBRA, A. S. B.. Integrated Acousto-Optical Temperature Sensor. Fiber And Integrated Optics, v. 6, n. 25, p.387-402, 2006.

[19] LI, Q. et al. Demonstration of narrow-band acousto-optic tunable filters on dispersion enhanced single-mode fibers. IEEE Photonics Technol. Lett**.**, n. 14, p.1351-1353, 2002.

[20] JUNG, Y., et al. Bandwidth control in a hybrid fiber acousto-optic filter. Optics Letters, n. 30, p. 84–86, 2005.

[21] MAZZALI, C.; FRAGNITO, H. L.. Optical PPM generator by direct-frequency shifting in Optical Fiber Communication Conference and Exhibit, 1998. OFC '98., Technical Digest WM13 n. 191, 1998.

[22] SOBRINHO, C. S., et al. Analysys of an Optical Logic Gate Using a Symmetric Coupler Operating With Pulse Position Modulation (PPM). Optics Communications, n. 281, p. 1056-1064, 2008.

[23] JACKEL, J. L., et al. Acousto Optic Tunable Filters (AOTF's) for multiwavelength optical cross conects: Crosstalk Considerations. J. Lightwave Technol., v. 14, p. 1056-1066.

[24] MIDWINTER, J. E.. Photonics in Switching**.** 2. ed. Academic Press, 1993.

[25] RAMASWAMI, R.; SIVARAJAN, K. N.. Optical Networks**.** Morgan Kaufmann Pub, 1998.

[26] ROBINSON, B.S.; MOORES, J.D.; MORIARTY, D.T. Pattern independent semiconductor-based interferometric all-optical switching using pulse-position modulation. Lasers and Electro-Optics, 2000. (CLEO 2000). Conference on Volume , Issue , p.690-691, 2000.

[27] C. A. Van Der Lubbe, Basic Methods of Cryptography, Faculty of Information Technology and Systems, Delft University of Technology, Cambridge University Press, 1999.

5 CONCLUSÃO

A quantidade de informação trocada diariamente por meios eletrônicos nos dias atuais pertence a uma escala gigantesca. Diante desse quadro, estudou-se a importância de métodos eficazes para a proteção desses dados enquanto são enviados de um usuário a outro. Por tratar-se de uma quantidade muito grande de dados, o processamento deve ocorrer de forma o mais rápida e eficientemente possível. É nesse contexto que surge o interesse de se conseguir dispositivos totalmente ópticos, funcionando como elementos capazes de tratar e/ou processar informação a velocidades ultra-rápidas.

Destarte, nos debruçamos sobre o estudo dos filtros acústico-ópticos sintonizáveis (AOTF) com guias de onda em substratos de niobato de lítio. O AOTF é um dispositivo que funciona a partir do princípio de interação acústico-óptica e tem atraído grande atenção, dentre outros aspectos, por ser provavelmente o único filtro capaz de selecionar múltiplos comprimentos de onda simultaneamente. Ele possui grande versatilidade em redes ópticas e, em particular, no estudo de chaveamento de energia a níveis ultra-rápidos. Realizamos um breve estudo numérico e analítico sobre tal dispositivo, onde foi possível destacar os efeitos de perda e não linearidade e, principalmente, foi possível observar os efeitos de biestabilidade e definir os parâmetros importantes para tal fenômeno.

Mostramos inicialmente as curvas de transmissão para os modos eletromagnéticos TE e TM, onde pudemos comprovar que a melhor transmissão ocorre quando $\Delta\beta = 0$ com $\kappa\xi_L = \pi/2$. Observamos que para valores diferentes desses, a transmissão cai significativamente. O efeito na freqüência é o acentuado estreitamento de banda. Quando os efeitos de não-linearidade e perda são considerados, novas modificações ocorrem nesses perfis. Estudamos vários modelos de não-linearidade e os efeitos de cada modelo estudado puderam ser vistos com detalhes.

Após o estudo numérico do AOTF, desenvolvemos um estudo numérico das equações que descreviam o comportamento dos modos no interior do dispositivo e foi possível obter várias resultados já encontrados na literatura. Entretanto, muito material inédito pode também ser obtido. Uma parte desse material é o estudo a biestabilidade óptica no AOTF com pulsos ultracurtos. A biestabilidade óptica ocorre quando o efeito de não-linearidade em um material

causa uma curva de histerese na curva de transmissão de um dispositivo. Ou seja, um dispositivo biestável é aquele que possui capacidade de gerar duas saídas diferentes para uma dada entrada. Todo dispositivo desse tipo possui a combinação de um componente não-linear e alguma forma de realimentação (***feedback***). Usamos pulsos ultracurtos em um AOTF, introduzindo um circuito de realimentação, a partir de uma das saídas do AOTF, induzindo variações no transdutor de onda acústica (SAW), que por sua vez, passaria a modificar o índice de refração do cristal que compões o meio em que os modos se propagam. Mostramos as curvas de biestabilidade em função do produto da constante de acoplamento (κ) pelo comprimento do dispositivo (ξ_L) e do fator de conversão potência-constante de propagação (G).

Para o estudo da biestabilidade óptica é necessário escolher apenas uma polarização na saída do dispositivo e é esta mesma polarização que irá receber a realimentação. A polarização escolhida foi a TE. Mostrou-se inicialmente que a quantidade de energia de saída contida no modo TE e no modo TM variam quando o produto $\kappa\xi_L$ assume valores diferentes. A curva de histerese foi apresentada para os valores de $\kappa\xi_L = 1.2$ e $G = 100$ e demonstrada a ocorrência da biestabilidade passou-se a estudar sua relação com esses parâmetros. Para condições nas quais a intensidade da potencia transmitida aumenta mais rapidamente que a da incidente, a resposta não-linear do meio pode ser usado para ganho diferencial. Nessa situação, uma pequena modulação da luz incidente pode ser convertida a uma grande modulação de luz transmitida. A gama de valores para a potência de entrada em que a potência de saída possui dois valores foi o que chamamos de intervalo da biestabilidade. Mostrou-se que esse intervalo varia significativamente tanto com G como com $\kappa\xi_L$, mas suas contribuições são diferentes.

Nas simulações apresentadas, foi possível observar que a variação do produto $\kappa\xi_L$ aumenta diretamente o tamanho do intervalo da biestabilidade. Como exemplo, para $\kappa\xi_L = 1.2$, o intervalo da biestabilidade óptica varia de algo em torno de 6.4 a 7.6W (uma variação de 1.2 W) enquanto que para $\kappa\xi_L = 1.4$, varia de 6.5 a 12.2W (uma variação de 4.7). O aumento de G, por sua vez, faz com que a biestabilidade ocorra em potências críticas de subida cada vez menores. A diferença entra a intensidade da potência de saída também é regulada através desse parâmetro; quanto maior G, menor a potência de saída. Para a completa compreensão desses fenômenos trabalhos futuros ainda precisam ser realizados, nos

quais o fenômeno da realimentação deve ser estuda com mais profundidade. Trabalhos futuros também precisam descobrir quais outros fatores poderiam influenciar esta biestabilidade. Tudo isso vai ajudar a entender melhor o comportamento das curvas biestáveis no dispositivo discutido.

Outra parte inédita obtida em nossos estudos, foi o que diz respeito ao uso do AOTF como criptografo. Discutimos inicialmente a importância dos métodos criptográficos para a proteção de mensagens numa rede óptica. Apresentamos alguns modelos clássicos e após discutir a importância da criptografia para sistemas totalmente ópticos para os meios de comunicação atuais, expusemos o modelo que nos propúnhamos estudar. Assim, fazendo uso das propriedades do AOTF somadas à modulação de pulsos ultracurtos por posição e amplitude simultaneamente, foi possível gerar um dispositivo que criptografasse pulsos ópticos (portando informações) e lançasse com segurança por uma rede. A técnica é utilizada para codificar pulsos ultracurtos sólitons (2ps), que se consiste basicamente em duas partes: a primeira é a redução do número de pulsos formando a mensagem original, através da modulação simultânea por posição e por amplitude. A cada quatro pulsos a formar a mensagem original, o processo de modulação reduzirá a quantidade para dois. Fizemos isso da seguinte forma: os dois primeiros pulsos serão polarizados no modo TE e os dois segundos no modo TM. O primeiro pulso de cada modo servirá para a modulação PAM e o segundo para a modulação PPM. Após esse processo, esses pulsos passam através de um AOTF. Apenas um dos modos eletromagnéticos será lançado através da fibra como um pulso de informação. Ou seja, a informação de quatro pulsos será condensada em apenas um. O processo de recuperação se dá pela passagem por um segundo AOTF usando a chave correta para a recuperação dos quatro pulsos de informação iniciais. O processo de codificação passa então a ser definido a partir de um par de parâmetros relacionados com os parâmetros usados nas modulações, é o que chamamos de par PPM/PAM (ε_{PPM} ,ε_{PAM}).

A segurança de tal dispositivo com respeito ao ataque ao sistema por usuários mal intencionados é então simulada e analisada. Observamos então que o modelo de criptografia proposto é resistente aos ataques sugeridos por intrusos que desejavam obter informações destinadas a outros usuários da rede. Após apresentar o funcionamento do dispositivo, foi necessário definir para quais valores de pares PPM/PAM ele realmente funcionaria. Discutiu-se que certas considerações, com relação à própria natureza do funcionamento do AOTF,

iriam invalidar certos grupos de chaves, de forma que definimos mais precisamente quais seriam.

Dessa forma, o produto cartesiano entre os conjuntos dos valores de ε_{PPM} (o intervalo contínuo que vai de 0.2 a 1) e de ε_{PAM} (o intervalo contínuo de 0.2 a 0.5) cria uma região em que é possível analisar a validade do funcionamento do dispositivo para o par PPM/PAM. O funcionamento do dispositivo somente é possível com a intersecção dessas regiões para os dezesseis tipos distintos de entradas de quatro **bits**. Essa região foi então definida e nesses pontos o dispositivo funciona com sucesso.

Esse trabalho abre, portanto, uma ampla discussão, uma vez que demonstra teoricamente a possibilidade de tal processo criptográfico. Diversos trabalhos deverão ser realizados no sentido de definir os efeitos nas regiões de funcionamento do dispositivo quando consideradas algumas características nas fibras da rede que liga o criptógrafo ao decriptógrafo. Podemos considerar perdas, não-linearidade, amplificação dos pulsos, etc.. Enfim, há aqui uma imensa quantidade de trabalho que ainda precisa ser desenvolvido até o ponto em que o problema sairá do âmbito teórico e passará para o prático. É preciso analisar como cada um desses efeitos agirá sobre a chave a ser utilizada e quais modificações as chaves deverão sofrer para que ainda funcionem corretamente. Entretanto, o modelo simulado nos deixa confiantes, uma vez que acreditamos que os efeitos citados não destruirão por completo as regiões de validade para o funcionamento do dispositivo. Assim, acreditamos poder dizer que a criptografia com pulsos ultracurtos a partir do uso de um AOTF e da modulação simultânea por amplitude e por posição se mostrou uma idéia realizável e bastante promissora dada a intensa busca atual por sistemas que funcionem num domínio totalmente óptico.

APÊNDICE: PRODUÇÃO CIENTÍFICA NO PERÍODO

Trabalhos Diretamente Ligados à Tese

Artigos

Optical Cryptography Under PPM-PAM Modulation Based in Short Optical Pulses in an Acoustic-Optic Tunable Filter (AOTF).
K. D. A. Sabóia, C. S. Sobrinho, A. C. Ferreira, W. B. Fraga, J.W.M. Menezes, M.L.Lyra** and A. S. B. Sombra
Submetido ao Microwave and Optical Technology Letters (julho 2009) (Submetido)

Optical Bistability in an Acoustic-Optic Tunable Filter (AOTF) Operating With Short Optical Pulses
K. D. A. Sabóia, F. T. Lima, A. C. Ferreira, C. S. Sobrinho, W. B. Fraga, J.W.M. Menezes and A. S. B. Sombra

Submetido ao Journal of Modern Optics (Novembro 2009) (Submetido)

Optical Bistability in an Acoustic-Optic Tunable Filter (AOTF) Operating With Short Optical Pulses

Congressos

Modulação de pulsos ultracurtos por amplitude e posição em um filtro acúicto-óptico sintonizavel.
K.D.A Sabóia, S.P. Marciano, A.S.B. Sombra
Proc. Do XXV Encontro dos Fisicos do Norte-Nordeste,
Outubro 15-20 Natal-RN – Brazil (2007).

Utilização de filtro acústico-óptico sintonizável como codificador-decodificador de pulsos ultracurtos
K.D.A Sabóia, J.S. Almeida , J.W.M. Meneses , W.B. Fraga, A.C. Ferreira, C.S. Sobrinho, A.M. Melo, J.C. Sales, G.F. Guimarães, A.F.G.F. Filho, H.O. Rodrigues, S.P. Marciano, A.S.B. Sombra
Proc. Do XXXI Encontro Nacional de Física da Matéria Condensada Maio 5-9, Águas de Lindóia-SP – Brazil (2008).

Optical Cryptography Under PPM/PAM Modulation Based in Short Optical Pulses in an Acoustic Optic Tunable Filter.

K.D.A. Sabóia, C.S. Sobrinho, A.C. Ferreira, W.B. Fraga, J.W.M. Menezes, H.T. Girão, A.S.B. Sombra

Proc. do XXXII Encontro Nacional de Física da Matéria Condensada, 11 a 15 de maio, Águas de Lindóia-SP – Brazil (2009).

Patentes

Uso de Filtros Sintonizáveis Acústico-Ópticos para Criptografia de Pulsos Ultracurtos. K. D. A. Saboia, A. C. Ferreira, C. S. Sobrinho, A. S. B. Sombra

Patente depositada no INPI com protocolo 012090000953 em 09/12/2009.

Outros

Artigos

A Performance Study of Logical Gate Using PPM Optical Pulse Modulation for TDM Systems.
C. S. Sobrinho, C. S. N. Rios, S. P. Marciano, G.F. Guimarães, J. C. Sales, K.D.A. Sabóia, H.H.B. Rocha and A. S. B. Sombra.
Optics Communications Volume 275 (2) (2007) 476-485 (Elsevier)

Logic Gates Based in Two and Three-MOdes Nonlinear Optical Fiber Couplers.
J. W. M. Menezes, W. B. de Fraga, A. C. Ferreira, K. D. A. Saboia, A. F. G. F. Filho, G. F. Guimarães, J. R. R. Sousa, H. H. B. Rocha and A. S. B. Sombra
Optical and Quantum Electronics 39 (14) (2007) 1191-1206 (Springer)

Analysis of na Optical Logic Gate Using a Symmetric Couler Operating with Pulse Position Modulation (PPM).
C. S. Sobrinho, A. C. Ferreira, J. W. M. Menezes, G. F. Guimarães, W. B. Fraga , A. F. G. F. Filho, H. H. B. Rocha, S. P. Marciano, K. D. A. Sabóia and A. S. B.Sombra Optics Communications 281(5) (2008) 1056-1064 (Elsevier Science B.V.)

Optical Short Pulse Switching Characteristics of Ring Resonators.
J. L. S. Lima, K. D. A. Sabóia, J. C. Sales, J.W.M. Meneses, W.B. Fraga, G.F. Guimarães and A. S. B. Sombra
Optical Fiber Technology 14(1)(2008) 79-83 (Elsevier Science B.V.)

Numerical Analysis of the stability of optical bullets (2+1) in a Planar Waveguide with Cubic-Quintic Nonlinearity.
W. B. Fraga, J.W.M. Menezes, C.S.Sobrinho, A.C. Ferreira, G. F. Guimarães, A.W.Lima Jr., A.F.G.F.Filho, H.H.B. Rocha, K.D. Saboia, F.T.Lima, J.M.S.Filho, A.S.B.Sombra.
Optical and Quantum Electronics 41(2) (2009)121-130 (Springer)

Periodic modulation of nonlinearity in a fiber Bragg grating: a numerical investigation.
A. F. de Morais Neto A. F. G. Furtado Filhob, H. H. B. Rocha, G. F. Guimarães,
K. D. A. Saboia and A. S. B. Sombra
Submetido ao Optics Communications (setembro 2006) (Submetido)

Congressos

Short Puls Switching in Optical Ring Resonators.
J.L.S. Lima, K.D.A. Sabóia, J.C. Sales, E.F. de Almeida, A.S.B. Sombra
Proc. do XXIX Encontro Nacional de Física da Matéria Condensada, 09 a 13 de maio, São Lourenço, MG (2006)

Livros Grátis

(http://www.livrosgratis.com.br)

Milhares de Livros para Download:

Baixar livros de Literatura
Baixar livros de Literatura de Cordel
Baixar livros de Literatura Infantil
Baixar livros de Matemática
Baixar livros de Medicina
Baixar livros de Medicina Veterinária
Baixar livros de Meio Ambiente
Baixar livros de Meteorologia
Baixar Monografias e TCC
Baixar livros Multidisciplinar
Baixar livros de Música
Baixar livros de Psicologia
Baixar livros de Química
Baixar livros de Saúde Coletiva
Baixar livros de Serviço Social
Baixar livros de Sociologia
Baixar livros de Teologia
Baixar livros de Trabalho
Baixar livros de Turismo