Distribuição Quântica de Chave Utilizando Modulação Não Linear

Francisco Revson F. Pereira, Edmar J. Nascimento, Francisco M. Assis

***Resumo*— Neste artigo, é investigado o uso de técnicas de modulação não linear nos protocolos de distribuição quântica de chaves com variáveis contínuas. Especificamente, procura-se relacionar a interferência do espião em um canal quântico com a probabilidade de anomalia definida nos esquemas de modulação não linear. Com isso, a probabilidade de anomalia pode ser usada para quantificar o conhecimento do espião sobre a informação transmitida.**

***Palavras-Chave*— Modulação não linear, modulação retorcida, distribuição quântica de chaves, criptografia quântica, estados coerentes, variáveis contínuas.**

***Abstract*— In this article, we apply non-linear modulation techniques to continuous variables quantum key distribution protocols. More specifically, we try to relate the interference of spying the quantum channel to the probability of anomaly defined in non-linear modulation schemes. In this way, the probability of anomaly can be used to quantify the spy's knowledge of the transmitted information.**

***Keywords*— Non-linear modulation, twisted modulation, quantum key distribution, quantum cryptography, coherent states, continuous variables.**

I. INTRODUÇÃO

O uso da criptografia quântica ou, mais especificamente, da Distribuição Quântica de Chaves (DQC) tem como objetivo a distribuição de uma chave secreta entre duas partes (Alice e Bob) para fins criptográficos. A segurança do processo não reside em hipóteses computacionais, mas em fundamentos da mecânica quântica, como a impossibilidade de se realizar cópias perfeitas de estados quânticos não ortogonais [1]. Mais de duas décadas após o protocolo pioneiro BB84 [2], vários protocolos para DQC foram implementados com sucesso, tanto em laboratório como em aplicações comerciais [3].

Atualmente, os protocolos para DQC podem ser implementados usando variáveis discretas ou contínuas. Nos protocolos com variáveis discretas, a informação é codificada usualmente na polarização ou na fase de fótons isolados. Por outro lado, nos protocolos com variáveis contínuas, a informação é codificada nas amplitudes de quadratura do campo eletromagnético quantizado [4], [5]. Uma das vantagens da abordagem com variáveis contínuas é que ela permite implementações mais simples, usando componentes ópticos convencionais [6].

Os protocolos para DQC com variáveis contínuas empregam em sua maioria estados gaussianos[1] [7]. Esses estados podem ser do tipo comprimido (*squeezed states*), coerentes ou térmicos. Dentre os diversos protocolos propostos, o protocolo com estados coerentes de Grosshans e Grangier (GG02) se destaca [8], [9]. Em linhas gerais, no protocolo GG02, Alice gera dois valores aleatórios x_A e p_A de acordo com uma distribuição gaussiana de média nula e variância $V_A N_0$. Em seguida, ela prepara um estado coerente $|x_A + ip_A\rangle$ e o envia para Bob. Este, por sua vez, escolhe aleatoriamente se mede a quadratura x ou a quadratura p através de uma medição homódina. Em seguida, há uma discussão pública através de um canal autenticado em que Bob informa a Alice em quais quadraturas as medidas foram feitas. Dessa forma, Alice descarta os valores que não são compatíveis com as medidas de Bob. Ao final do processo, Alice e Bob possuem uma sequência de variáveis aleatórias contínuas correlacionadas em que parte delas será usada para estimar os parâmetros do canal e a outra parte será usada para extrair uma sequência binária comum, a chave secreta. O processo se encerra com as etapas clássicas de reconciliação da informação e de amplificação de privacidade [10].

Tomando-se como base o protocolo GG02, Weedbrook *et al.* [11] mostraram que é possível realizar o protocolo medindo-se ambas as quadraturas. Ou seja, Bob pode usar um divisor de feixe no sinal recebido e medir a quadratura x em uma saída e a quadratura p na outra saída. A vantagem dessa variação é que Bob não necessita de um gerador aleatório para comutar entre as quadraturas a serem medidas. Do ponto de vista clássico, a preparação do estado coerente $|x_A + ip_A\rangle$ consiste na modulação de um feixe de luz coerente em amplitude e fase. Diferentes escolhas da amplitude e da fase permitem varrer o espaço de fase das variáveis x_A e p_A.

No paradigma clássico, modulações não lineares nos sistemas analógicos têm a vantagem de permitir uma diminuição no erro médio quadrático sem a necessidade de aumento na potência do sinal transmitido [12]. Uma desvantagem destes esquemas de modulação é a sensibilidade a níveis de ruído que ultrapassam um determinado limiar. Na ocorrência de tais eventos, verifica-se um distorção extrema no sinal demodulado, ou até mesmo a perda total do sinal. Essa grande distorção pode ser usada na DQC durante a etapa de estimação dos parâmetros do canal a fim de quantificar a presença de um espião.

Com base no que foi exposto, propõe-se neste artigo uma variação no protocolo de Weedbrook *et al.* aplicando-se os conceitos de modulação não linear (*non-linear modulation*) apresentados em [12]. A ideia é mapear uma variável aleatória gaussiana em uma curva bidimensional não linear, sendo os pontos desta curva correspondentes aos estados coerentes a serem preparados. Desta forma, a estrutura da curva é usada

Francisco Revson F. Pereira – Mestrando no Programa de Pós-Graduacão em Engenharia Elétrica, PPgEE/UFCG. Edmar J. Nascimento – Doutorando no Programa de Pós-Graduacão em Engenharia Elétrica, PPgEE/UFCG. Francisco M. Assis – Departamento de Engenharia Elétrica, UFCG, Campina Grande, Paraíba. Os autores são membros do Instituto de Estudos em Computação e Informação Quânticas. Emails:revson.ee@gmail.com, ejnascimento@ee.ufcg.edu.br, fmarcos@dee.ufcg.edu.br

[1]Estados cuja distribuição de Wigner é gaussiana.

para detectar a presença do espião e para melhorar a correlação entre as variáveis de Alice e Bob a serem reconciliadas.

O artigo está estruturado da seguinte forma. Na seção II é feito um resumo sobre os conceitos de modulação não linear usados neste artigo, bem como uma breve explanação sobre o efeito do limiar de ruído. Na seção III são discutidos alguns aspectos relevantes ao entendimento dos protocolos para DQC com variáveis contínuas. Na seção IV é apresentado o protocolo proposto pelos autores deste artigo, bem como os resultados de simulações numéricas realizadas. Por fim, na seção V são tecidas considerações a respeito deste trabalho e de trabalhos futuros.

II. Modulação Não Linear

Seja o sistema de comunicação ilustrado na figura 1, em que uma variável aleatória contínua m é transmitida através de um canal AWGN (*Additive White Gaussian Noise*). O ruído, representado por $n(t)$, tem densidade espectral de potência $N_0/2$. Para cada mensagem m, o transmissor produz a forma de onda descrita por

$$s_m(t) = s_1(m)\varphi_1(t)+s_2(m)\varphi_2(t)+\cdots+s_N(m)\varphi_N(t), \quad (1)$$

em que $\varphi_i(t), i = 1,\cdots,N$ são portadoras ortogonais com energia unitária e $s_j(m), j = 1,\cdots,N$ é a parametrização de $s_m(t)$ na base $\{\varphi_i(t)\}$. O receptor gera uma estimativa da mensagem, $\hat{m}$, a partir do sinal recebido $r(t)$. O desempenho do sistema de comunicação é medido pelo erro quadrático médio $\overline{\epsilon^2}$ entre a mensagem transmitida $m(t)$ e a sua estimativa $\hat{m}(t)$.

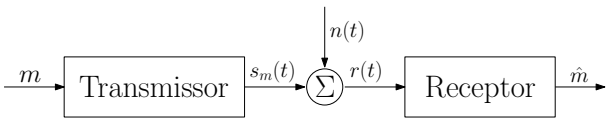

Fig. 1. Diagrama de blocos do sistema de comunicação considerado

A partir da equivalência entre sinais e vetores, o sinal transmitido $s_m(t)$ pode ser representado como um vetor em $\Re^N$ na base $\{\varphi_i(t)\}$ como

$$\vec{\boldsymbol{s}}_m \quad = \quad [s_1(m), s_2(m), \cdots, s_N(m)]. \quad (2)$$

Em modulações não lineares, quando $m(t)$ varia ao longo de sua faixa de valores, $\vec{\boldsymbol{s}}_m$ varia ao longo de uma curva, conforme ilustrado na figura 2 para $N = 2$. O receptor usando uma decodificação por máxima verossimilhança (ML - *Maximum Likelihood*) decide pelo ponto da curva mais próximo do vetor recebido $\vec{\boldsymbol{r}}$. Ou seja,

$$\hat{m}(t) = \arg_m \min |s_m(t) - r(t)|. \quad (3)$$

A. Aproximação de Baixo Nível de Ruído

Quando o nível de ruído é baixo, a decisão do receptor ML pode ser aproximada da maneira seguinte [12]. Admitindo-se que o parâmetro de entrada do modulador, m, tenha assumido um valor m_0 de forma que $\vec{s}_m = \vec{s}_0$ e que a densidade de ruído é pequena, a um nível que a probabilidade de que o ponto recebido $\vec{r}$ esteja próximo a $\vec{s}_0$ seja próxima de um. Para esse caso, é possível fazer uma aproximação de primeira ordem sobre o sinal recebido em torno do ponto de interesse, ou seja,

$$\vec{s}_m \approx \vec{s}_0 + (m - m_0)\dot{\vec{s}}_0, \quad (4)$$

com

$$\dot{\vec{s}}_0 = \frac{d\vec{s}_m}{dm}\Big|_{m=m_0}. \quad (5)$$

Localmente, com essa aproximação, o problema se torna similar ao da modulação linear. Com o ruído gaussiano branco, o receptor ML escolhe $\hat{m}$ para m de forma que $|\vec{r} - \vec{s}_m|$ seja o mínimo possível. Pela hipótese de ruído fraco, é possível desprezar a probabilidade de $\vec{r}$ estar em uma região que não esteja próxima do verdadeiro valor transmitido. Na vizinhança de $\vec{r}$, a possível região geométrica do sinal recebido se assemelha a um alongamento da região do sinal transmitido por um fator $|\dot{\vec{s}}_0|$. Assim, o erro quadrático médio condicional é dado por

$$E[(m - \hat{m})^2 | m = m_0] \approx \frac{N_0/2}{|\dot{\vec{s}}_0|^2}. \quad (6)$$

Como a magnitude quadrática de um vetor é igual à sua energia, aplicando-se a relação de Parseval, tem-se que

$$|\dot{\vec{s}}_0|^2 = \int_{-\infty}^{\infty} \Big[\frac{\partial s_m(t)}{\partial m}\Big]^2_{m=m_0} dt. \quad (7)$$

Quando o lado direito dessa igualdade é independente de m, é possível definir o fator de alongamento S como sendo

$$S^2 = \int_{-\infty}^{\infty} \Big[\frac{\partial s_m(t)}{\partial m}\Big]^2 dt \quad (8)$$

Com essa hipótese de independência, após se tirar a média de 6 sobre a distribuição de m, o erro quadrático médio é dado por

$$\overline{\epsilon^2} = \frac{N_0/2}{S^2}. \quad (9)$$

A partir dessa expressão, pode-se observar que o erro quadrático médio pode ser reduzido aumentando-se o fator de alongamento S, que, por sua vez, é proporcional ao comprimento da curva L.

B. Observações sobre o Limiar do Ruído

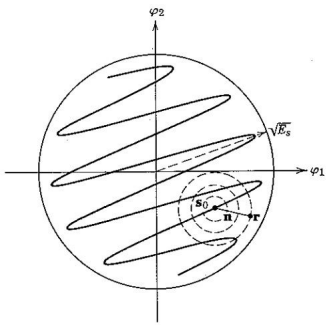

Fig. 2. Lugar geométrico do sinal para o qual a análise linear se torna inválida. Fonte: [12]

À medida que o nível de ruído aumenta, a aproximação linear de primeira ordem não é mais válida. Através da

observação da figura 2, pode-se observar que os pontos recebidos podem ser decodificados em outras regiões da curva. Considerando-se que a curva que descreve a possível modulação do sinal esteja confinada em uma esfera de dimensionalidade fixa e raio $\sqrt{E_s}$, observa-se que o comprimento da curva não pode ser aumentado indefinitivamente sem que dois pontos de dobras diferentes estejam muito próximos. Assim, quando o comprimento L da curva aumenta indefinitivamente enquanto E_s e $N_0/2$ são mantidos constantes, vários pontos da curva se aproximam, de forma que a probabilidade de que um ponto recebido seja detectado em outras regiões da curva aumenta. Essa probabilidade é denominada de probabilidade de anomalia e está ligada ao efeito de limiar que ocorre nas modulações não lineares. Se ela excede um determinado valor, o desempenho do sistema deteriora fortemente. Tal situação pode ser ilustrada na figura 3, em que a saída $\hat{m}$ do receptor ML salta discontinuamente quando o vetor recebido $\vec{r}$ se move continuamente entre os pontos ρ_1 e ρ_2.

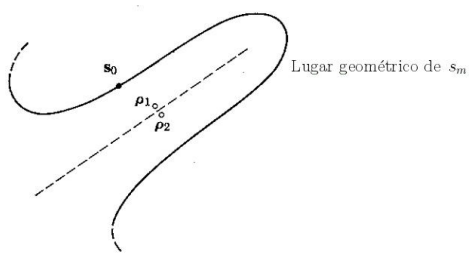

Fig. 3. Quando $\boldsymbol{r} = \boldsymbol{\rho}_1$, o ponto $\boldsymbol{s}_m$ de menor distância a $\boldsymbol{r}$ é próximo a $\boldsymbol{s}_0$, fazendo com que $\hat{m}$ seja quase igual a m. Isto não é verdade quando $\boldsymbol{r} = \boldsymbol{\rho}_2$. Fonte: [12]

III. Variáveis Contínuas em Óptica Quântica

Na transição para o mundo da mecânica quântica, quantidades observáveis como a posição e o momento de uma partícula passam a ser representadas por operadores não comutativos. Na óptica quântica, os modos eletromagnéticos quantizados podem ser caracterizados pelo modelo do oscilador harmônico quântico fazendo-se a massa igual a um [4]. As quadraturas dos modos desempenham o papel dos operadores posição e momento do oscilador, obedecendo assim a uma relação análoga à da incerteza de Heisenberg [5]. Essa propriedade é fundamental para a DQC com variáveis contínuas.

A. Sistemas Bosônicos

Um sistema quântico é chamado de sistema de variáveis contínuas quando tem um espaço de Hilbert com espectro de dimensão infinita. Os sistemas de interesse são representados por N modos bosônicos[2], correspondendo a N modos quantizados de radiação do campo eletromagnético. Em geral, os N modos bosônicos são associados a um produto tensorial de espaços de Hilbert $\mathcal{H}^{\otimes N} = \otimes_{k=1}^{N}\mathcal{H}_k$, correspondendo a N pares de operadores bosônicos $\{\hat{a}_k, \hat{a}_k^\dagger\}$, os quais são chamados de operadores de destruição e criação, respectivamente.

[2]Bósons são partículas que seguem a estatística de Bose-Einstein. O exemplo mais comum são os fótons.

O espaço de Hilbert deste sistema é separável e de dimensão infinita. Cada modo bosônico pode ser expandido em uma base contável $\{|n\rangle\}_{n=0}^{\infty}$, chamada de base de Fock ou de estados número. Essa base é composta por autoestados do operador número $\hat{N} := \hat{a}^\dagger\hat{a}$, i.e., $\hat{N}\,|n\rangle = n\,|n\rangle$. Sobre esses estados, a ação dos operadores bosônicos é bem definida, sendo determinada pela relação de comutação bosônica. Em particular, tem-se

$$\hat{a}\,|0\rangle \;=\; 0,\ \hat{a}\,|n\rangle = \sqrt{n}\,|n-1\rangle\ \ (n \geq 1) \qquad (10)$$

$$\hat{a}^\dagger\,|n\rangle \;=\; \sqrt{n+1}\,|n+1\rangle\ \ (n \geq 0). \qquad (11)$$

Além dos operadores bosônicos, o sistema bosônico pode ser descrito por outros tipos de operadores de campo. Esses operadores são denominados de operadores de quadratura, $\{\hat{x}_k, \hat{p}_k\}_{k=1}^{N}$, que podem ser definidos como[3]

$$\hat{x}_k \;:=\; \hat{a}_k + \hat{a}_k^\dagger,\ \hat{p}_k := i(\hat{a}_k^\dagger - \hat{a}_k). \qquad (12)$$

Os operadores de quadratura representam observáveis canônicos sem dimensão do sistema e atuam similarmente aos operadores posição e momento do oscilador harmônico quântico.

É importante frisar que os operadores quadratura são observáveis com espectro contínuo. De fato, os dois operadores tem autoestados

$$\hat{x}\,|x\rangle \;=\; x\,|x\rangle\,,\ \hat{p}\,|p\rangle = p\,|p\rangle\,, \qquad (13)$$

com autovalores contínuos $x \in \Re$ e $p \in \Re$. Os autoestados $|x\rangle$ e $|p\rangle$ identificam duas bases que são conectadas por uma transformação de Fourier.

O significado dos operadores de quadratura pode ser melhor ilustrado observando-se um modo do campo elétrico, cujo operador é dado por

$$\hat{E}_k(\mathbf{r}, t) \;=\; E_0[\hat{x}_k \cos(\omega_k t - \mathbf{k}.\mathbf{r}) + \hat{p}_k \sin(\omega_k t - \mathbf{k}.\mathbf{r})].$$

Nesta expressão, pode-se notar que $\hat{x}_k$ representa a componente em fase e $\hat{p}_k$ a componente em quadratura do campo elétrico quando a referência de fase é $\cos(\omega_k t - \mathbf{k}.\mathbf{r})$.

Como foi mencionado anteriormente, os protocolos para DQC com variáveis contínuas empregam estados gaussianos. Desses, o mais importante é o estado do vácuo $|0\rangle$. O vácuo satura a relação de Heisenberg para os operadores de quadratura e além disso, as variâncias desses operadores são iguais. No caso da notação escolhida, ambas tem variância iguais a um. Como o vácuo é interpretado como a ausência de fótons, a incerteza sobre ele é conhecida como ruído do vácuo ou *quantum shot noise*.

A partir do vácuo, pode-se obter um estado coerente aplicando-se a ele um operador de deslocamento, que é definido por

$$D(\alpha) := \exp(\alpha a^\dagger - \alpha^* a), \qquad (14)$$

sendo $\alpha = x_0 + ip_0$ uma amplitude complexa. Aplicando-se esse operador, é gerado o estado coerente $|\alpha\rangle = D(\alpha)\,|0\rangle$. Ele tem a mesma variância do vácuo, mas com valores médios dados por (x_0, p_0). Esta propriedade pode ser observada na

[3]Esta definição é consistente com a notação $\hbar = 2$. Outras definições podem ser encontradas.

figura 4, na qual o vácuo e um estado coerente são representados por círculos com diâmetro unitário. Os estados coerentes podem ser expandidos na base de Fock como

$$|\alpha\rangle = \exp\Big(-\frac{1}{2}|\alpha|^2\Big)\sum_{n=0}^{\infty}\frac{\alpha^n}{\sqrt{n!}}|n\rangle\,. \quad (15)$$

Além disso, dois estados coerentes com diferentes amplitudes complexas são não ortogonais.

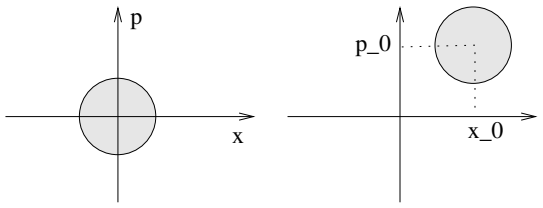

Fig. 4. Na esquerda, tem-se a representação do vácuo, enquanto na direita, um estado coerente.

IV. Protocolo e Simulações

Na abordagem adotada em [9] para o protocolo GG02, Alice gera um estado coerente $|x_A + ip_A\rangle$, com x_A e p_A escolhidos de acordo com uma distribuição gaussiana de média nula e variância $V_A N_0$ (N_0 o ruído do vácuo). O estado gerado pode ser caracterizado pelas variáveis x_{in} e p_{in} com distribuição gaussiana com média nula e variância $VN_0 = (V_A+1)N_0$. O espião utiliza uma máquina de cópia entrelaçadora (*entangling cloner*), cujas entradas x_{in} e p_{in} resultam nas saídas x_E e p_E para o espião (Eva) e nas saídas x_B e p_B para Bob. Nesse caso, o canal do ponto de vista de Bob pode ser caracterizado por:

$$\begin{aligned}
x_B &= \sqrt{G_x}x_{in} + \sqrt{G_x}B_x, && (16)\\
p_B &= \sqrt{G_p}p_{in} + \sqrt{G_p}B_p, && (17)\\
\langle x_{in}^2\rangle &= \langle p_{in}^2\rangle = VN_0 = (V_A+1)N_0, && (18)\\
\langle x_{in}B_x\rangle &= \langle p_{in}B_p\rangle = 0, && (19)\\
\langle B_x^2\rangle &= \chi_x N_0,\ \langle B_p^2\rangle = \chi_p N_0. && (20)
\end{aligned}$$

Nestas expressões, G representa o ganho do canal ($0 \leq G \leq 1$) e χ o ruído equivalente na entrada em unidades de N_0. Em protocolos com medição em apenas uma quadratura, χ é composto por uma contribuição do vácuo $\chi_{vac} = (1-G)/G$ e do excesso de ruído ϵ, que depende da ação do espião e do aparato de detecção. Por outro lado, nos protocolos em que ambas as quadraturas são medidas, χ ainda possui uma terceira componente $1/G$ devido à ação do divisor de feixe.

Admitindo-se que o canal atua da mesma forma em ambas as quadraturas, ou seja, $G_x = G_p = G$ e $\chi_x = \chi_p = \chi$ e que Bob mede ambas as quadraturas aplicando um divisor de feixe 50:50, tem-se que as quadraturas medidas por Bob são caracterizadas por:

$$\begin{aligned}
x_B &= \sqrt{\frac{G}{2}}(x_{in}+B),\ p_B = \sqrt{\frac{G}{2}}(p_{in}+B), && (21)\\
\langle B^2\rangle &= \chi N_0 = [\frac{1-G}{G} + \epsilon + \frac{1}{G}]N_0, && (22)\\
\langle x_B^2\rangle &= \frac{G}{2}(\langle x_{in}^2\rangle + \langle B^2\rangle)\\
&= \frac{1}{2}(G\langle x_{in}^2\rangle + (1-G)N_0 + G\epsilon N_0 + N_0), && (23)\\
\langle p_B^2\rangle &= \frac{G}{2}(\langle p_{in}^2\rangle + \langle B^2\rangle)\\
&= \frac{1}{2}(G\langle p_{in}^2\rangle + (1-G)N_0 + G\epsilon N_0 + N_0). && (24)
\end{aligned}$$

A. Protocolo Proposto

O protocolo proposto neste artigo utiliza estados coerentes, assim como o GG02, e medições heteródinas, como em [7]. A sua peculiaridade está na representação da informação usada para gerar os estados quânticos. Ao invés de gerar os valores das quadraturas diretamente a partir de uma distribuição de probabilidade, o que se propõe é que esses valores sejam gerados a partir de uma curva referente a um tipo de modulação não linear, assim como descrito na seção II. Com isso, o protocolo consiste nas seguintes etapas:

1) Alice escolhe um valor m de uma distribuição gaussiana p_m com média nula e variância V_m;
2) Alice mapeia m em uma curva bidimensional resultando nas coordenadas x_A e p_A;
3) Alice prepara o estado coerente $|x_A + ip_A\rangle$ e o envia a Bob;
4) Bob mede ambas as quadraturas do estado coerente recebido, obtendo as quadraturas x_B e p_B;
5) Bob aplica o critério da distância mínima a fim de obter um ponto na curva (x'_B, p'_B) tal que $(x_B - x'_B)^2 + (p_B - p'_B)^2$ seja mínimo;
6) Alice e Bob selecionam um conjunto de valores x_A, p_A e x_B, p_B a fim de estimar os parâmetros do canal e calcular a probabilidade de anomalia;
7) Se a probabilidade de anomalia for superior a um valor acordado, o protocolo é abortado, caso contrário, Bob usa o restante dos dados para obter $\hat{m}$;
8) Alice e Bob usam os protocolos de reconciliação da informação e de amplificação de privacidade para extrair uma chave secreta comum das variáveis aleatórias correlacionadas m e $\hat{m}$.

B. Simulações

Para simular a probabilidade de anomalia para o protocolo proposto, utiliza-se como curva não linear a espiral de Arquimedes uniforme [13]. Isto faz com que parametrização feita por Alice na segunda etapa do protocolo seja dada por

$$x_A = Am\cos(k_p|m|),\ p_A = -Am\sin(k_p|m|), \quad (25)$$

em que A é um fator ganho e k_p é uma constante que mede o desvio da modulação em relação à fase. Na curva de Arquimedes uniforme, a distância entre duas curvas próximas

é dada por $2\pi/k_p$, o que leva a probabilidade de anomalia no processo de medida ser dada pela expressão

$$P_{\text{Anomalia}} = 2\int_{\frac{\pi}{k_p}}^{\infty} \frac{1}{\sqrt{2\pi N_T}} \exp\left(\frac{-x^2}{2N_T}\right), \qquad (26)$$

em que N_T representa a variância do ruído no estado de Bob.

Nas simulações realizadas, considerou-se um canal sem atenuação ($G = 1$). Com isso, as expressões apresentadas nas equações (21-24) são simplificadas. Particularmente, o termo de ruído passa apenas a ter a contribuição do excesso de ruído ϵ e do divisor de feixe na medida. Considerou-se também $N_0 = 1$ e ϵ variando de 0 a 1. A equação (26) foi usada para obter um parâmetro k_p compatível com as probabilidades de anomalia usadas na simulação. Para um valor de $k_p = 2\pi/3$, tem-se na figura 5 a evolução da probabilidade de anomalia à medida que ϵ é aumentado.

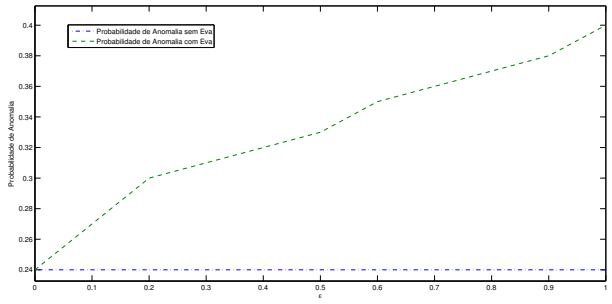

Fig. 5. Probabilidade de anomalia para os casos em que $\epsilon = 0$ (reta constante) e para os casos em que ϵ varia (curva ascendente).

Como é notado na figura 5, a probabilidade de anomalia é uma alternativa para a detecção do espião. Ela cresce com o aumento da ação de Eva sobre o estado transmitido, aqui representado pelo excesso de ruído ϵ. A partir de uma análise de segurança, é possível adotar um valor mínimo para a probabilidade de anomalia a fim de que o espião possua menos informação sobre o estado transmitido do que Alice para Bob e assim, se possa gerar uma chave secreta.

V. Considerações Finais

Não foi realizado neste artigo uma análise de segurança do protocolo considerado. O mapeamento em uma curva não linear restringe a gama de valores possíveis para x_A e p_A, sugerindo uma possível estratégia de ataque usando discriminação de estados como a que foi feita em [14] para um protocolo semelhante ao GG02, mas com quatro estados apenas [15]. Essa questão de segurança será investigada em trabalhos futuros.

Outro ponto a ser investigado é a comparação com outros protocolos em condições similares. Sabe-se que um dos grandes gargalos dos protocolos para DQC com variáveis contínuas está no processo de reconciliação. Em especial quando as distâncias aumentam e por consequência o ruído também (a componente do vácuo), se faz necessário usar processos de reconciliação com códigos extremamente longos a fim de se conseguir extrair informação das variáveis de Alice e Bob [10]. É de se esperar que a estrutura não linear da curva proporcione uma maior imunidade ao ruído, facilitando assim o processo de reconciliação.

Agradecimento

Os autores agradecem à FINEP pelo apoio financeiro através do projeto RENASIC-QUANTA.

Referências

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.*, vol. 74, pp. 145–195, Mar 2002. [Online]. Available: http://link.aps.org/doi/10.1103/RevModPhys.74.145

[2] C. H. Bennett and G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing," in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*. New York: IEEE Press, 1984, pp. 175–179.

[3] L. Oesterling, D. Hayford, and G. Friend, "Comparison of commercial and next generation quantum key distribution: Technologies for secure communication of information," in *Homeland Security (HST), 2012 IEEE Conference on Technologies for*, Nov 2012, pp. 156–161.

[4] M. Fox, *Quantum Optics: An Introduction*. Oxford University Press, 2006.

[5] S. L. Braunstein and P. van Loock, "Quantum information with continuous variables," *Rev. Mod. Phys.*, vol. 77, pp. 513–577, Jun 2005. [Online]. Available: http://link.aps.org/doi/10.1103/RevModPhys.77.513

[6] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Rev. Mod. Phys.*, vol. 81, pp. 1301–1350, Sep 2009. [Online]. Available: http://link.aps.org/doi/10.1103/RevModPhys.81.1301

[7] C. Weedbrook, S. Pirandola, R. Garcia-Patron, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, "Gaussian quantum information," *Rev. Mod. Phys.*, vol. 84, pp. 621–669, May 2012. [Online]. Available: http://link.aps.org/doi/10.1103/RevModPhys.84.621

[8] F. Grosshans and P. Grangier, "Continuous variable quantum cryptography using coherent states," *Phys. Rev. Lett.*, vol. 88, p. 057902, Jan 2002. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevLett.88.057902

[9] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, "Quantum key distribution using gaussian-modulated coherent states," *Nature*, vol. 421, pp. 238–241, Jan. 2003.

[10] G. V. Assche, *Quantum Cryptography and Secret-Key Distillation*. Cambridge University Press, 2006.

[11] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, "Quantum cryptography without switching," *Phys. Rev. Lett.*, vol. 93, p. 170504, Oct 2004. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevLett.93.170504

[12] J. M. Wozencraft and I. M. Jacobs, *Principles of Communication Engineering*. Waveland Pr. Inc., 1990.

[13] R. G. Cavalcante and R. Palazzo Junior, "Análise de curvatura de modulações não lineares associadas a curvas." in *XXVI Simpósio Brasileiro de Telecomunicações 2008 (SBrT2008)*, Rio de Janeiro, Brazil, Sep. 2008.

[14] P. Huang, J. Fang, and G. Zeng, "State-discrimination attack on discretely modulated continuous-variable quantum key distribution," *Phys. Rev. A*, vol. 89, p. 042330, Apr 2014. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevA.89.042330

[15] A. Leverrier and P. Grangier, "Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation," *Phys. Rev. Lett.*, vol. 102, p. 180504, May 2009. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevLett.102.180504