Protocolo para Autenticação Quântica de Mensagens Clássicas Utilizando Variáveis Contínuas

Francisco Revson F. Pereira, Elloá B. Guedes, Francisco M. Assis

***Resumo*— Ao considerar a autenticação quântica de mensagens, é necessário considerar as particularidades deste cenário ao conceber protocolos e a analisar a segurança dos mesmos, pois as regras da Mecânica Quântica precisam ser levadas em consideração. Considerando este contexto, o presente trabalho tem por objetivo apresentar um protocolo de autenticação quântica de mensagens utilizando variáveis contínuas. Segundo o protocolo proposto, é possível restringir, até um limiar desejado, a quantidade de informação que é acessível a um espião deste sistema de comunicação. Os resultados em termos de segurança deste protocolo podem ser comparados com resultados relevantes existentes na literatura.**

***Palavras-Chave*— Autenticação Quântica de Mensagens; Variáveis Contínuas; Mecânica Quântica.**

***Abstract*— When considering the authentication of quantum messages, we must take into account the particularities of this scenario when conceiving protocols and when their security is analyzed, because the laws of Quantum Mechanics must be respected. Considering this context, this work aims at presenting a quantum protocol for message authentication that makes use of continuous variables. According the proposed protocol, it is possible to restrict, up to a certain lower bound, the amount of accessible information to an eavesdropper of this communication system. In terms of security, the results of this protocol are aligned with relevant results in the literature.**

***Keywords*— Quantum Message Authentication; Continuous Variables; Quantum Mechanics.**

I. Introdução

A *Mecânica Quântica* é o ramo da física que estuda os fenômenos em sua escala nanoscópica. Sistemas de comunicação quânticos transmitem informação usando sistemas físicos, tais como átomos e fótons, que são descritos pelas leis da Mecânica Quântica. De acordo com estas leis, a informação pode estar representada de duas formas: discreta e contínua.

A descrição da informação de maneira discreta é adotada em função da simplificação do modelo matemático de representação. A descrição de acordo com variáveis contínuas também é passível de ser utilizada, embora requeira um maior domínio matemático. Exemplos de sistemas quânticos de variáveis contínuas incluem modos quantizados de sistemas bosônicos, tais como os diferentes graus de liberdade do campo eletromagnético, modos de vibração de sólidos, entre outros. Em virtude deles serem uma descrição quântica do campo eletromagnético, que é a entidade que mais usual de transmissão de informação em comunicações, isto implica que sistemas quânticos de variáveis contínuas sejam particularmente relevantes para a comunicação, detecção e criptografia quânticas.

O uso das variáveis quânticas contínuas já se estende por diversas áreas da Teoria da Informação, Comunicação e Criptografia. Porém, ainda não foi verificado a adoção destas variáveis no estudo de sistemas de autenticação de mensagens. No escopo de criptografia quântica, em particular, a autenticação é um ingrediente essencial em diversos sistemas de comunicação. No caso de uma troca quântica de chaves, por exemplo, os participantes legítimos em determinado momento precisam transmitir algumas amostras dos bits que foram obtidos do protocolo, precisam calcular os erros de transmissão e também detectar, sempre que possível, a existência de um espião. Porém, quando realizam estas tarefas, o espião pode vir a interceptar a troca de mensagens e se passar por uma das partes legítimas, o que seria uma grave falha de segurança. Para evitar que isto aconteça, há que se adotar protocolos de autenticação.

Levando em consideração a importância da autenticação em cenários quânticos, este trabalho tem com objetivo propor um protocolo de autenticação de mensagem utilizando variáveis quânticas contínuas, em particular, utilizando estados comprimidos. Como consequência da utilização deste protocolo, é possível conceber um sistema de autenticação que impossibilite o espião de obter mais informação do que se deseja, isto é, a informação acessível por este é limitada. Este resultado é comparado aos resultados alcançados por Assis et al. [1].

O artigo está estruturado da seguinte forma. Na Seção II é apresentada uma fundamentação teórica sobre autenticação quântica de mensagens, incluindo uma descrição detalhada do protocolo de Assis et al. [1]. Na Seção III são discutidos alguns aspectos relevantes sobre variáveis contínuas no domínio quântica. Na Seção IV, o protocolo proposto e os seus elementos são caracterizados, incluindo aspectos vantajosos de sua utilização e também uma análise entrópica do mesmo. Por fim, considerações finais e sugestões de trabalhos futuros são apresentadas na Seção V.

II. Autenticação Quântica de Mensagens Clássicas

Autenticação é uma área bastante estudada pela Criptografia Clássica. No caso de uma única mensagem, o objetivo da autenticação é assegurar ao destinatário que a mensagem é originária de um remetente em particular. No caso de uma interação em curso, dois aspectos estão envolvidos: primeiramente, em um momento inicial, o objetivo é assegurar que duas partes são autênticas, isto é, que elas são quem afirmam

Francisco Revson F. Pereira – Mestrando no Programa de Pós-Graduacão em Engenharia Elétrica, PPgEE/UFCG. Elloá Barreto Guedes – Escola Superior de Tecnologia, Universidade do Estado do Amazonas, Manaus, Amazonas. 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, elloa.uea, fmarassis}@gmail.com

ser; após isto, deve ser assegurado que a comunicação não sofra interferências de tal modo que um espião possa se passar por uma das partes legítimas, com o intuito de realizar transmissões ou recepções não-autorizadas [2].

Com o intuito de prover estas características, a autenticação deve ser realizada sob dois aspectos:

1) **Autenticação de Origem de Dados**. Permite que o destinatário verifique que uma mensagem não foi alterada "em trânsito" e que origina de um certo remetente;
2) **Autenticação de Identidade**. Permite ao destinatário verificar se um remetente é quem afirma ser. Se alguns aspectos de segurança são garantidos, também permite ao destinatário verificar que ninguém se passou pelo remetente verdadeiro.

Para ilustrar como a autenticação funciona, considera-se um modelo de autenticação por chave simétrica em que um remetente (Alice), um destinatário (Bob) e uma espiã (Eva) encontram-se ilustrados na Figura 1. O objetivo neste modelo é garantir a Bob que uma mensagem autêntica foi enviada por Alice. Para tanto, em um momento inicial Alice e Bob compartilham uma chave secreta k que será utilizada para autenticação. Alice cifra a mensagem original m com a chave k usando um algoritmo E, produzindo $m_c = E(m, k)$ (Passo 1). Alice envia m_c para Bob por um canal inseguro que está sendo espionado por Eva (Passo 2). Assume-se que Eva pode observar toda informação transmitida entre Alice e Bob e que, em geral, Eva conhece a mensagem original m, mas não a chave k utilizada para cifrá-la.

Existem dois tipos de ataques que podem ser realizados pela espiã: o *ataque de representação*, no qual Eva envia uma mensagem esperando que ela seja aceita por Bob como sendo uma mensagem originária de Alice; e o *ataque de substituição*, no qual Eva observa a mensagem cifrada transmitida e a substitui por uma outra mensagem.

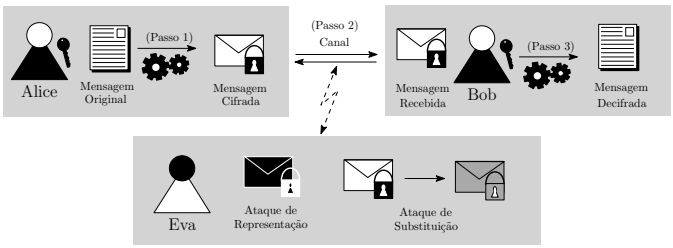

Fig. 1. Modelo de Autenticação por Chave Simétrica.

Ao receber a mensagem, Bob irá usar a chave k e um algoritmo de decifragem D para tentar recuperar a mensagem original, isto é, ele irá fazer $D(m_c, k)$ (Passo 3). Se nenhum ataque ocorreu, Bob irá obter o par $\langle m, 1\rangle$, em que m é a mensagem original enviada por Alice e 1 indica que a autenticação foi bem sucedida. Caso contrário, Bob deve descartar o que recebeu e solicitar a Alice um novo envio [3], [4].

No cenário quântico, apesar do objetivo ser o mesmo, alguns passos da autenticação são diferentes do caso clássico. Isso acontece porque a informação é considerada como sendo *física* e, por esta razão, comporta-se conforme as leis da Mecânica Quântica. Como consequência, os *protocolos quânticos de autenticação* devem obedecer tais leis físicas que definem como representar e trocar informação.

Para enviar uma mensagem m para Bob de acordo com um protocolo quântico de autenticação, Alice deve codificar m com um certo código antes de enviá-la. Porém, se o mesmo código é sempre usado, Eva pode simplesmente criar erros que o código não pode detectar, prejudicando a comunicação entre as partes legítimas. Em virtude disto, Alice e Bob devem usar uma família de códigos que detectem diferentes tipos de erro. A chave k agora diz qual código será usado. Uma vez que Eva não conhece k, ela não sabe quais erros o código pode detectar e, não importa o que ela faça, há uma alta probabilidade dela ser descoberta. Além disso, Alice e Bob devem também cifrar o estado quântico com o intuito de evitar modificações no estado quântico causadas por Eva [5].

Autenticação quântica possui um papel importantíssimo na Criptografia Quântica, pois ela precede a execução dos *protocolos quânticos de distribuição de chaves* (QKD – *Quantum Key Distribution*). Tais protocolos permitem que as partes produzam uma chave secreta e restrita, que pode ser usada para cifrar e decifrar mensagens [6]. Uma vez que os protocolos QKD requerem uma autenticação prévia e considerando o crescente sucesso dos mesmos em implementações em longas distâncias [7], muitos protocolos quânticos de autenticação foram recentemente propostos na literatura [8]–[16].

A. Protocolo de Autenticação de Assis et al.

No escopo deste trabalho, será considerado o protocolo de autenticação proposto por Assis et al. [1], cujo propósito é promover a autenticação de origem de dados de mensagens clássicas por meio de canais quânticos. O esquema proposto por estes autores é ilustrado na Figura 2.

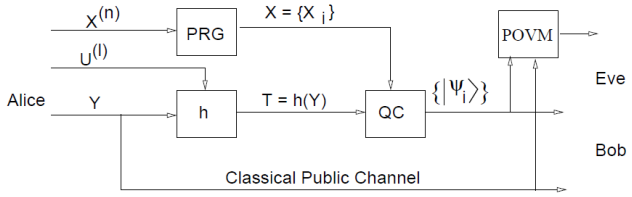

Fig. 2. Protocolo de Autenticação de Mensagens Clássicas via Canais Quânticos de Assis et al. [1]

Neste protocolo, tem-se que a variável aleatória $U^{(l)}$ especifica uma certa função *hash* universal , $X^{(n)}$ é a semente para um gerador de números pseudo-aleatórios e Y denota uma mensagem arbitrária que Alice deseja enviar para Bob. A mensagem Y é enviada pelo canal clássico diretamente e será utilizada para verificar se a autenticação foi bem sucedida ou se resultou em falhas. Alice deve alimentar o gerador de números pseudo-aleatórios com $X^{(n)}$ que, neste caso, atua como semente, e aplicar à função hash especificada por $U^{(l)}$ em Y, produzindo uma *tag* $T = h(Y)$.

A partir daí, tem-se início uma codificação que irá produzir estados quânticos $\{|\psi_i\rangle\}$ que serão enviados pelo canal. Cada estado quântico $|\psi_i\rangle$ a ser criado depende do i-ésimo bit da tag (denotado por T_i) e do valor do gerador pseudo-aleatório (denotado por X_i). Se o gerador produziu o bit $X_i = 0$, então

será utilizada a base binária $B_0 = \{|0\rangle, |1\rangle\}$ para preparação do estado $|\psi_i\rangle$ a ser enviado pelo canal, da seguinte forma:

$$|\psi_i\rangle = \begin{cases} |0\rangle, & \text{se } T_i = 0; \\ |1\rangle, & \text{se } T_i = 1. \end{cases} \quad (1)$$

Se o bit produzido pelo gerador é $X_i = 1$, então será utilizada a base de Hadamard $B_1 = \left\{|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}, |-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}\right\}$ e o estado produzido será:

$$|\psi_i\rangle = \begin{cases} |+\rangle, & \text{se } T_i = 0; \\ |-\rangle, & \text{se } T_i = 1. \end{cases} \quad (2)$$

Após esta codificação, Bob recebe o estado separável $|\psi_Y\rangle^{\otimes k}$ por meio de um canal quântico sem ruído. Nota-se que é uma codificação em estados quânticos da *tag* produzida por Alice. Para decodificá-la, Bob utilizará medições via POVM. Em seguida, Bob também irá aplicar a função hash pré-fixada ao Y recebido pelo canal clássico. Se não houve interferência do espião, espera-se que estes resultados sejam iguais, permitindo comprovar a autenticidade da mensagem enviada. Utilizando este método eles obtiveram que a incerteza que Eva tem sobre o conhecimento da saída do gerador aleatório, mesmo conhecendo Y e Z, é igual a $H(X^k|Z^k, Y^k) = k(1 - S^*)$, para $S^* = -2\cos^2(\pi/8)\log(\cos(\pi/8)) - 2\log(\sin(\pi/8))\sin^2(\pi/8) = 0.4763$. Será mostrado que o protocolo proposto neste trabalho fornece um método de obtensão de um valor maior sobre esta incerteza.

III. Variáveis Contínuas em Ótica Quântica

Esta seção visa apresentar a utilização de variáveis contínuas na Ótica Quântica. Para tanto, os sistemas bosônicos serão apresentados na Seção III-A e um exemplo é ilustrado na Seção III-B.

A. Sistemas Bosônicos

Um sistema quântico é chamado de *sistema de variáveis contínuas* quando tem um espaço de Hilbert com espectro de dimensão infinita [17]. O espaço deste sistema é separável e de dimensão infinita [18]. Isto acontece porque o espaço de Hilbert de um único modo é expandido por uma base contável $\{|n\rangle\}_{n=0}^{\infty}$, chamado de *base de Fock* ou *estado número* [17], [19], [20], a qual é composta de autoestados do operador número $\hat{N} := \hat{a}^\dagger\hat{a}$, i.e., $\hat{N}|n\rangle = n|n\rangle$, os quais $\hat{a}$ e $\hat{a}^\dagger$ são chamados de *operadores de destruição e criação* [19], [20], respectivamente. Sobre estes estados, a ação dos operadores bosônicos é bem definida, sendo determinada pela relação de comutação bosônica. Em particular, tem-se

$$\hat{a}|0\rangle = 0, \ \hat{a}|n\rangle = \sqrt{n}|n-1\rangle \ (n \geq 1) \quad (3)$$

$$\hat{a}^\dagger|n\rangle = \sqrt{n+1}|n+1\rangle \ (n \geq 0). \quad (4)$$

Além dos operadores bosônicos, o sistema bosônico pode ser descrito por outro tipo de operadores de campo. Estes operadores são os operadores de quadratura do campo, $\{\hat{q}_k, \hat{p}_k\}_{k=1}^{N}$. O significado dos operadores de quadratura pode ser melhor ilustrado observando-se um modo do campo elétrico, cujo operador é dado por [19]

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

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 $\cos(\omega_k t - \mathbf{k}.\mathbf{r})$.

B. Exemplo de Estados Gaussianos

O estado gaussiano com que será utilizado no protocolo proposto, onde utiliza variáveis quânticas contínuas, é mostrado a seguir.

1) Estados Comprimidos: Quando se bombeia um cristal não linear com luz forte, alguns dos fótons bombeados com frequência $2w$ são divididos em dois pares de fótons com frequência w. O Hamiltoniano de interação deste processo contem termos $\hat{a}^{\dagger 2}$, relacionados com a geração de pares de fótons, e termos $\hat{a}^2$, termos que garantem a Hermiticidade do Hamiltoniano [19], [20]. A correspondente transformação Gaussiana unitária é o operador de compressão, no qual é definido, para o caso mono-modo, como sendo

$$S(r) := \exp[r(\hat{a}^2 - \hat{a}^{\dagger 2})/2], \quad (5)$$

onde $r \in \Re$ é chamado de parâmetro de compressão. Aplicando o operador de compressão no estado do vácuo gera-se um estado do vácuo comprimido [17], [19], [20]

$$|0, r\rangle = S(r)|0\rangle = \frac{1}{\sqrt{\cosh r}} \sum_{n=0}^{\infty} \frac{\sqrt{(2n)!}}{2^n n!} \tanh r^n |2n\rangle. \quad (6)$$

IV. Protocolo Proposto

Esta seção tem por objetivo apresentar um protocolo para autenticação em canais quânticos baseando-se na utilização de variáveis contínuas. A ideia deste protocolo é similar a de Assis et al. [1], descrita anteriormente na Seção II-A. A principal mudança consiste no processo da troca quântica de chaves, que não se baseia no protocolo BB84, mas sim na utilização de estados comprimidos [21], mostrados na Seção III-B.

Neste protocolo, as partes legítimas Alice e Bob estão conectadas via um canal quântico e também por um canal clássico público. Os valores da tag que Alice gera são binários e irão determinar qual o valor médio da quadratura escolhida para compressão deve assumir. Um codificador quântico (QC – *quantum coder*) recebe como entrada o valor da tag e a saída do gerador aleatório, esta última é utilizada no QC na parte de escolha entre duas regras de codificação, numeradas por $i \in \{0, 1\}$. O diagrama de blocos que representa este protocolo encontra-se ilustrado na Fig. 3.

A ideia da troca de chaves é a seguinte. De acordo com o princípio de Heisenberg [18], é impossível medir com precisão indefinida as duas quadraturas do campo elétrico monomodo, x e p. Isto fornece uma forma de codificação similar a do BB84, onde os elementos da chave $A_{T,i}$ são estados comprimidos ou em x (caso onde o gerador aleatório produz $X_i = 0$) ou em p (caso onde o gerador aleatório produz $X_i = 1$), de tal forma que o espião, sem saber qual das duas codificações foram usadas, não pode adquirir informação sem perturbar o estado [21]. Este é o ingrediente principal para proteger a chave de Eva, a espiã neste cenário.

Em particular, as duas regras de codificação são detalhadas da seguinte maneira:

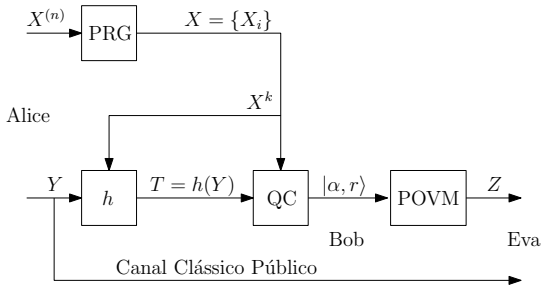

Fig. 3. Diagrama de Blocos do Protocolo de Autenticação de Mensagens Clássicas via Canais Quânticos Proposto.

- No caso 1, o gerador aleatório produziu uma saída $X_i = 0$. Alice prepara um estado comprimido do vácuo de forma que a flutuação de x seja comprimida em um fator $s_0 < 1$. Em seguida, ela aplica um deslocamento em x por uma quantidade igual a A_T, i. e., o valor médio de x será $\langle x \rangle = A_T$ assim, a regra de codificação de Alice é $A_{T,0} \rightarrow |A_T, s_0\rangle$. O valor médio que x assume depende da tag assim, x pode assumir os valores A_0 ou A_1, dependendo de qual é valor o valor de T.
- De forma similar, no caso 2 ($X_i = 1$), Alice envia um estado comprimido em p (i.e., com parâmetro de compressão $s_1 > 1$), posteriormente desloca p para o valor $A_{T,1}$. Tal regra de codificação é dada por $A_{T,1} \rightarrow |iA_T, s_1\rangle$.

Bob, o receptor deste estado quântico, mede x ou p, obtendo como resultado $Y_{B,x}$ ou $Y_{B,p}$, através de uma medição homódina [22], [23]. Esta medição homódina mede, com a precisão que ele deseje, uma das duas quadraturas, onde esta escolha da quadratura medida é feita aleatóriamente. Depois de enviar um número predefinido de estados comprimidos, Alice revela a Bob a regra de codificação para cada estado comprimido. Eles mantem apenas os elementos medidos nos quais as escolhas feitas por Alice e por Bob foram iguais, indicando que o resultado é conhecido por ambos mesmo que não seja explicitamente mencionado. Os valores medidos de Bob que restaram desse processo são denotados por Y_B.

Do ponto de vista de Eva, uma observadora não-autorizada, o estado enviado por Alice é visto como

$$\rho_1 = \frac{1}{\sqrt{2}} |A_0, s_1\rangle + \frac{1}{\sqrt{2}} |A_1, s_1\rangle , \tag{7}$$

para o caso 1 e

$$\rho_2 = \frac{1}{\sqrt{2}} |iA_0, s_2\rangle + \frac{1}{\sqrt{2}} |iA_1, s_2\rangle . \tag{8}$$

Como no protocolo BB84, a incerteza sobre qual foi o estado transmitido deve ser igual para ambos os casos, ou seja, $\rho_1 = \rho_2$ em termos de medida estatística. De acordo com Assche [24], é possível mostrar que esta condição é equivalente a ter

$$\Sigma_{T,0}^2 + \sigma_0^2 = \frac{1}{\sigma_1^2} \tag{9}$$

e

$$\Sigma_{T,1}^2 + \sigma_1^2 = \frac{1}{\sigma_0^2}, \tag{10}$$

o que pode ser resumido em

$$1 + \frac{\Sigma_{T,1}^2}{\sigma_1^2} = 1 + \frac{\Sigma_{T,2}^2}{\sigma_2^2} = \frac{s_2}{s_1}. \tag{11}$$

Observa-se que esta equação impõe que os valores que s_1 e s_2 devem assumir dependendo das variâncias relacionadas à compressão em cada caso considerado, $\Sigma_{T,1}$ e $\Sigma_{T,2}$, e das variâncias da fonte para cada caso, σ_1 e σ_2, que para o caso em que o gerador é aleatório são iguais a $\sigma_1 = \sigma_2 = 1/4$.

A. Análise Entrópica

Será mostrado que o protocolo proposto fornece uma forma de maximixar a incerteza sobre a saída do gerador aleatório $X = X_i$ da Fig. 3 quando comparado com o resultado mostrado por Assis et al. [1]. Para isso, serão consideradas duas situações: (i) quando há um bloco que contém apenas um elemento; e (ii) quando há blocos de tamanho k. Para ambas as situações, serão consideradas as entradas $X \sim Ber(\frac{1}{2})$.

1) Bloco de Tamanho Unitário: Como o objetivo de Eva é maximizar o conhecimento de X, então ela deseja minimizar a entropia $H(X|Y, Z)$. Para o caso em questão, será mostrado que essa entropia é $H(X|Z, Y) \geq 1 - S_{\text{comprimido}}$, onde

$$S_{\text{comprimido}} = \log_2(1 + 2\overline{n}), \tag{12}$$

para $\overline{n}$ sendo o número médio de fótons do estado comprimido enviados pelo canal.

Teorema 1: A incerteza sobre X dados Z e Y, seguindo os elementos da Fig.3, é igual a

$$H(X|Z, Y) \geq 1 - S_{\text{comprimido}} = H^*, \tag{13}$$

em que $S_{\text{comprimido}}$ é mostrado na Eq. 12.

Demonstração: É possível mostrar [25] que a informação mútua, $I(X; Z|Y)$, é maximizada por

$$I(X; Z|Y) \leq S_{\text{comprimido}} = \log_2(1 + 2\overline{n}) \tag{14}$$

em que $\overline{n}$ é o número médio de fótons do operador densidade transmitido pelo QC. Esta quantidade é saturada quando se tem uma das duas quadraturas com incerteza muito inferior a da outra, i. e., quando o estado está muito comprimido.

Como $H(X|Z, Y) = H(X|Y) - I(X; Z|Y)$ e $H(X|Y) = 1$, pois X é independente de Y e X tem distribuição binária uniforme, então a incerteza mínima que Eva pode obter sobre X é dada por

$$H(X|Y, Z) \geq H^*, \tag{15}$$

onde é adotado $H^* := 1 - S_{\text{comprimido}}$. ■

De acordo com este teorema, é possível afirmar que a espiã Eva, mesmo tendo acesso à mensagem Y e a variável Z, que é resultado da medida sobre o estado comprimido, ela ainda tem uma incerteza maior ou igual a H^*. Quando comparado ao trabalho de Assis et al. [1], nota-se uma liberdade em um parâmetro ajustável experimentalmente, que é o número médio de fótons do estado comprimido, de forma que a incerteza que Eva possui sobre a saída do gerador aleatório pode assumir o valor desejado para cada aplicação, isto não é possível no protocolo de Assis et al. [1]. Na Fig. 4 é possível visualizar a variação de H^* para diversos valores de $\overline{n}$.

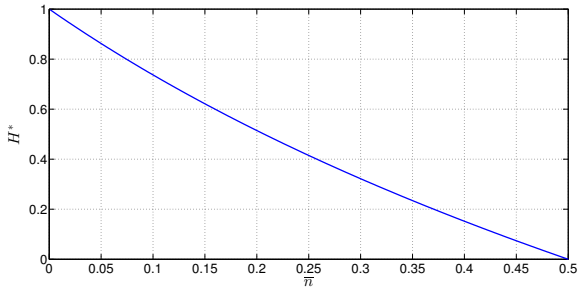

Fig. 4. H^* em termos do número médio de fótons do estado comprimido $\overline{n}$

2) Bloco de Tamanho k: Para esse novo caso, o estado que Eva obtém é

$$\rho_{Y^k} = \bigotimes_{i=1}^{k} \left(\frac{1}{\sqrt{2}} |Y, s_1\rangle + \frac{1}{\sqrt{2}} |Y, s_2\rangle \right). \quad (16)$$

Esta equação implica no teorema a seguir.

Teorema 2: A incerteza sobre o bloco X^k dado Y^k e Z^k é dado por

$$H(X^k|Y^k, Z^k) \geq kH^* \quad (17)$$

Demonstração: Inicialmente, observe que

$$H(X^k|Y^k, Z^k) = H(X^k) - I(X^k; Z^k|Y^k). \quad (18)$$

Notando que o produto tensorial de estados que são enviados pelo canal pode ser separável, então

$$I(X^k; Z^k|Y^k) = kI(X; Z|Y) \leq kS(\rho_{\text{comprimido}}). \quad (19)$$

E, de forma similar ao caso anterior, tem-se que $H(X^k) = k$. Juntando essas informações, obtém-se

$$H(X^k|Y^k, Z^k) \geq k(1 - S(\rho_{\text{comprimido}})) = kH^*. \quad (20)$$

■

Neste segundo caso, tem-se também que a incerteza de Eva sobre a chave trocada entre os participantes legítimos admite uma liberdade no seu valor dependendo do parâmetro $\overline{n}$ do estado comprimido.

V. Considerações Finais

Neste trabalho foi apresentado um protocolo de autenticação de mensagem que faz uso de variáveis quânticas continuas. O sistema utilizado para a realização do protocolo foi baseado no trabalho de Assis et al. [1], mas com mudanças relevantes na codificação a ser realizada, que agora passa a transmitir estados comprimidos pelo canal.

Em comparação com o trabalho no qual se baseia, o protocolo apresentado mostra-se mais robusto em relação à espionagem, pois há uma diminuição da informação acessível na saída do gerador. A depender do número médio de fótons transmitido pelo canal, este ganho pode fazer com que a informação acessível ao espião seja mais adequado em cenários práticos.

Em trabalhos futuros, almeja-se considerar diferentes modelagens no canal quântico de informações, considerando erros e perdas, por exemplo. Além disso, almeja-se introduzir a utilização de geradores pseudo-aleatórios.

Agradecimentos

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

Referências

[1] F. M. Assis, A. Stojanovic, P. Mateus, , and Y. Omar, "Improving classical authentication over a quantum channel," *Entropy*, vol. 14, pp. 2531–2549, 2012.

[2] W. Stallings, *Cryptography and Network Security – Principles and Practices*, P. Hall, Ed. Prentice Hall, 2005.

[3] H. Delfs and H. Knebl, *Introduction to Cryptography – Principles and Applications*, Springer, Ed. Springer, 2007.

[4] H. C. van Tilborg, *Encyclopedia Of Cryptography and Security*, Springer, Ed. Springer, 2005.

[5] H. Barnum, C. Crepeau, D. Gottesman, A. Smith, and A. Tapp, "Authentication of quantum messages," in *43rd Annual IEEE Symposium on the Foundations of Computer Science (FOCS '02)*. IEEE Press, 2002, pp. 449–458.

[6] M. A. Nielsen and I. L. Chuang, *Computação Quântica e Informação Quântica*, C. U. Press, Ed. Bookman, 2005.

[7] R. J. Hughes, G. L. Morgan, and C. G. Peterson, "Quantum key distribution over a 48km optical fiber network," *J. Mod. Opt*, vol. 47, p. 533, 2000.

[8] L. Yang, L. Hu, and D.-G. Feng, "Quantum message authentication based on classical np-complete problem," arXiv.org: quantum-ph/0310078, 2003.

[9] M. Curty and D. J. Santos, "Quantum authentication of classical messages," *Physical Review A*, vol. 64, pp. 062 309–1–06 230–5, 2001.

[10] X. Li and D. Zhang, "Quantum information authentication using entangled states," in *International Conference on Digital Telecommunications*, 2006.

[11] Y. Kanamori, S.-M. Yoo, D. A. Gregory, and F. T. Sheldon, "Authentication protocol using quantum superposition states," *International Journal of Networks Security*, vol. 9, pp. 101–108, 2009.

[12] G. Zeng and G. Guo, "Quantum authentication protocol," arXiv.org :quant-ph/0001046, 2000.

[13] X. Li and H. Barnum, "Quantum authentication using entangled states," *International Journal of Foundations of Computer Science*, vol. 15, pp. 609–617, 2004.

[14] Y. S. Zhang, C. F. Li, and G. C. Guo, ""quantum authentication using entangled state," arXiv.org : quant-ph/0008044, 2000.

[15] H. N. Barnum, "Quantum secure identification using entanglement and catalysis," arXiv.org: quantum-ph/9910072, 1999.

[16] G. Zeng and W. Zhang, "Identity verification in quantum key distribution," *Physical Review A*, vol. 61, pp. 022 303–1–022 303–5, 2000.

[17] C. Gerry and P. Knight, *Introductory Quantum Optics*. Cambridge University Press, 2004.

[18] J. J. Sakurai and J. J. Napolitano, *Modern Quantum Mechanics*. Addison-Wesley, 2010.

[19] R. Loudon, *The Quantum Theory of Light*. Oxford University Press, 2000.

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

[21] G. van Assche, *Quantum Cryptography and Secret-Key Distillation*. Cambridge University Press, 2012.

[22] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, "Gaussian quantum information," *REVIEWS OF MODERN PHYSICS*, 2012.

[23] J. Proakis and M. Salehi, *Digital Communications*. McGraw-Hill Science/Engineering/Math, 2007.

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

[25] Y. Yamamoto and H. A. Haus, "Preparation, measurement and information capacity of optical quantum states," *Rev. Mod. Phys.*, vol. 58, pp. 1001–1020, 1986.