Novo protocolo de reconciliação de chaves secretas geradas quanticamente utilizando códigos LDPC no sentido Slepian-Wolf

Laryssa Mirelly Carvalho de Araújo, Francisco Marcos de Assis e Bruno Barbosa Albert

***Resumo*— Este artigo apresenta uma solução alternativa ao uso das funções *Slice* para reconciliação de variáveis aleatórias contínuas em um contexto de geração de chaves secretas para fins de criptografia. O protocolo de reconciliação proposto baseia-se na função distribuição de probabilidade das variáveis aleatórias e se mostra um método competitivo por sua capacidade de gerar a mesma quantidade de *bits* que o esquema atualmente em uso, com uma vantagem de menor iteratividade. O processo de correção de erros é feito com base no uso de códigos LDPC a partir de uma compressão da sequência de *bits* a ser utilizada como chave, fundamentado no teorema de Slepian-Wolf, minimizando a informação vazada pelo canal clássico – assumido perfeito – para um possível espião que observa o canal.**

***Palavras-Chave*— Reconciliação de chaves secretas; LDPC; Slepian-Wolf.**

***Abstract*— This article presents an alternative solution to the use of the Slice functions to reconcile continuous random variables in a secret key generation context for encryption purposes. The proposed reconciliation protocol is based on the probability distribution function of the random variables and shows a competitive method for its ability to generate the same amount of bits as the scheme currently in use, with a lower iterativity. The process of error correction is performed based on the use of LDPC codes from a compression of the sequence of bits to be used as key, based on the Slepian-Wolf theorem, minimizing the information leaked through the classic channel – assumed perfect – for a possible spy who observes the channel.**

***Keywords*— Secret Key Reconciliation; LDPC; Slepian-Wolf.**

I. Introdução

A criptografia trata do problema de realizar comunicação ou computação envolvendo duas ou mais partes que podem ou não confiar uns nos outros, através de técnicas de codificação de mensagens voltadas à proteção da informação que estas contêm [16]. Para que duas partes legítimas, Alice e Bob, se comuniquem sob sigilo é necessário que estas façam uso de um algoritmo para cifrar e decifrar suas mensagens e de uma chave secreta que, se de comprimento idêntico ao da mensagem a ser trocada e utilizada uma única vez, garante segurança incondicional ao criptossistema de chave privada conforme demonstrado por Claude Shannon [15].

Entretanto, inerente a tais criptossistemas está o problema de distribuição de chaves, que deve ser conhecida apenas pelas partes legítimas. Neste cenário, a distribuição quântica de chaves (QKD – *Quantum Key Distribution*) surge como uma solução promissora para fins de compartilhamento de uma chave secreta através de propriedades não-clássicas de estados quânticos com a ajuda de um canal de comunicação clássico autenticado auxiliar, que pode ser utilizada para troca de informações sigilosas [11]. A segurança da QKD se baseia, fundamentalmente, no fato de que medições de variáveis incompatíveis inevitavelmente afeta o estado do sistema quântico, de modo que, com a informação codificada em variáveis incompatíveis, a espionagem se torna mensurável, logo, a existência de um espião que observa o canal quântico enquanto Alice e Bob tentam compartilhar uma chave é perceptível como uma perturbação no canal de comunicação e os *bits* da chave estabelecidos enquanto da presença do espião podem ser descartados [16], [1]. Nesse esquema de distribuição de chaves, as partes legítimas possuem uma vantagem sobre um possível espião (Eva): a capacidade de conversarem através de um canal clássico autenticado para combinarem uma chave comum, descartando o conhecimento de Eva sobre a mesma [1].

A estrutura desse artigo está organizada da seguinte forma: a seção II aborda as etapas de um protocolo de distribuição quântica de chaves a partir do uso de variáveis contínuas. Na seção III é apresentado o novo método de quantização proposto em contrapartida ao protocolo mais amplamente utilizado: o *Sliced Error Correction* (SEC). Na seção IV é exposto o método de correção de erros utilizado para obtenção de sequências binárias idênticas com elevada probabilidade para Alice e Bob a partir de um esquema de compressão de fonte com intuito de limitar ainda mais a informação vazada para Eva. Na seção V são exibidos os resultados para o novo método de quantização através da probabilidade de erro e da capacidade de cada canal e, ainda, através da correção de erros a partir do uso de códigos LDPC em um esquema de compressão de fontes, para que a quantidade de *bits* trocados pelo canal clássico (assumido perfeito) seja a menor possível. A seção VI expõe as considerações finais acerca do trabalho realizado, assim como o objeto de estudo para trabalhos futuros.

II. Distribuição Quântica de Chaves Secretas utilizando Variáveis Contínuas

A primeira etapa para implementação de um protocolo CV-QKD (*Continuous Variable Quantum Key Distribution*) consiste na fase de comunicação quântica, na qual há a geração

Laryssa Mirelly Carvalho de Araújo, Francisco Marcos de Assis e Bruno Barbosa Albert, Centro de Engenharia Elétrica e Informática, Universidade Federal de Campina Grande, Campina Grande-PB, E-mails: laryssa.araujo@ee.edu.ufcg.br, fmarcos@dee.edu.ufcg.br, albert@dee.edu.ufcg.br. Este trabalho foi financiado pela CAPES.

e transmissão de distribuições aleatórias de estados coerentes: Alice gera dois números aleatórios x_A e p_A com distribuição gaussiana e variância σ_X^2 e envia o estado coerente $|x_a + ip_A\rangle$ para Bob que, por sua vez, escolhe aleatoriamente medir uma das duas quadraturas X ou P; através do canal clássico, fazendo uso de um esquema de autenticação para garantir que Eva não modificou as mensagens, ele informa a Alice sobre o observável que utilizou nas medições para que os erros provenientes de escolhas de bases diferentes sejam descartados. Após a fase quântica, as partes legítimas compartilham duas sequências de realizações de variáveis aleatórias gaussianas correlacionadas [9].

Apesar de se trabalhar com estados quânticos contínuos como portadoras de informação, tanto a chave secreta quanto as mensagens de reconciliação podem ser feitas discretas por essa abordagem apresentar uma série de vantagens conforme apresentado em [1], de modo que, uma fase de quantização das sequências de números reais compartilhadas por Alice e Bob se faz necessária.

Uma vez que o canal quântico não é livre de ruído, estes não compartilham sequências idênticas, logo, a pequena quantidade de erros na *string* de Bob é corrigida na fase de reconciliação. Como Eva tem a possibilidade de modificar mensagens durante essa fase, Alice e Bob devem autenticá-la. Após a reconciliação, estes compartilham uma *string* idêntica com elevada probabilidade mas que não pode ser utilizada como uma chave devido ao fato de que a informação de Eva deve ser considerada – ela adquire informação durante a correção de erros e talvez durante a transmissão quântica [5]. Assim, Alice e Bob devem mapear suas *strings* através de uma função em um subconjunto menor, de modo a diminuir a informação de Eva sobre a chave a quase zero. Esse estágio é chamado amplificação de privacidade após o qual Alice e Bob compartilham uma chave secreta conhecida apenas entre si.

III. Quantização da Chave Bruta

A. SEC

O protocolo SEC foi proposto em [1] como um esquema genérico de reconciliação para fontes não-binárias usando códigos de correção de erros binários, para o qual uma importante aplicação é a correção de variáveis aleatórias Gaussianas correlacionadas, $X \sim N(0, \Sigma^2)$ e $Y = X + \epsilon$ com $\epsilon \sim N(0, \sigma^2)$, com X e Y definidas nos conjuntos $\mathcal{X}$ e $\mathcal{Y}$.

A discretização dos valores é feita a partir de funções de fatiamento, $S(x)$, que levam do espaço da chave bruta de Alice, $\mathcal{X}$, para GF(2); um vetor de funções de fatiamento $S_{1\cdots m}(x) = (S_1(x), ..., S_m(x))$ é assim definido quando mapeia os elementos de chave bruta de Alice em dígitos binários, ou seja, $K(x) = S_{1\cdots m}(x)$, de modo que o alfabeto discreto tem tamanho máximo 2^m.

Cada um dos estimadores

$$\tilde{S}_1(y), \tilde{S}_2(y, S_1(x)), \cdots, \tilde{S}_m(y, S_1(x), \cdots, S_{m-1}(x)) \quad (1)$$

por sua vez, define um mapeamento do espaço da chave bruta de Bob e das funções de fatiamento de Alice de índices menores em GF(2) e é utilizado por Bob para adivinhar $S_i(X)$ com conhecimento de Y e dos *bits* previamente corrigidos, tratando-se, portanto, de um processo extremamente iterativo e complexo devido à necessidade de se otimizar as funções $S_i(X)$ para maximizar a informação mútua entre os t intervalos escolhidos no conjunto dos reais, $T(X)$, e a sequência possuída por Bob, Y, para que em seguida seja possível a associação de m valores binários a esses intervalos de modo que as fatias possam ser corrigidas com tão pouca informação vazada quanto possível.

Assim, a realização de x do valor contínuo X do lado de Alice deve ser mapeado por T no valor $T(x)$ da chave tal que

$$T(x) = arg \min_{k=1}^{t} D(P_{Y|X=x} || P_{Y|K=k}) \quad (2)$$

ou seja, para o k cuja distribuição $P_{Y|K=k}$ seja o vizinho mais próximo de $P_{Y|X=x}$ em termos da distância KL. Portanto, o mapeamento $T(X)$ é definido através das distribuições $P_{Y|K=k}$ que, por sua vez, dependem de $T(X)$. Por conseguinte, é necessário um algoritmo no qual o mapeamento e as probabilidades condicionais sejam atualizadas alternadamente [1].

B. Quantização pela função distribuição de probabilidade

Com foco na reconciliação de sequências de realizações de variáveis aleatórias gaussianas correlacionadas, é proposto um novo esquema de quantização que leva em consideração a função distribuição de probabilidade das variáveis gaussianas enviadas por Alice e recebidas por Bob, de modo a contornar as dificuldades do protocolo atualmente empregado.

Da Teoria da Informação, extrai-se o lema apresentado em [6] sobre o qual se baseia a ideia para nova solução de discretização das chaves brutas:

***Lema**:* Seja X uma variável aleatória com função de distribuição contínua $F(x)$, defina $U = F(X)$. Então, U é uniforme em $[0, 1]$.

Como resultado direto do lema enunciado, a função distribuição contínua da variável aleatória X leva os valores do espaço da chave bruta de Alice, $\mathcal{X}$, no intervalo $[0, 1]$ com distribuição uniforme, isto é, os *bits* resultantes da expansão binária de $F(X)$ são Bernoulli($\frac{1}{2}$), de modo que formam uma representação comprimida da sequência X.

A expansão binária

$$x = 0.x_1x_2\cdots x_{l_i} = \sum_{j=1}^{l_i} x_j 2^{-j} \quad (3)$$

de números no intervalo $[0, 1]$ apresenta o formato $0.F_1F_2\cdots F_l$, onde cada realização $F_i \in GF(2)$, $1 \leq i \leq l$, com probabilidades iguais para as saídas 0 e 1, e l correspondendo ao número de *bits* escolhido para representar a variável contínua.

Propõe-se, portanto, a quantização das sequências de realizações de variáveis aleatórias gaussianas correlacionadas compartilhadas por Alice e Bob por meio de quatro passos:

1) Calcular o valor da função distribuição de probabilidade para cada realização de X e de Y, correspondendo a um valor no intervalo entre 0 e 1;

2) Realizar a expansão binária deste valor, obtendo valores no formato $0.F_1F_2\cdots F_l$;
3) Utilizar a sequência binária após o ponto como a representação binária de cada x_i ou y_i;
4) Definir os canais BSC como as realizações de cada variável aleatória de Bernoulli $F_1,\ F_2,\ \cdots,\ F_l$, isto é, dado o vetor de r realizações da variável aleatória gaussiana de Alice e a matriz $l \times r$ que representa a quantização desses valores em l *bits*, os canais são representados pelas linhas da matriz mostrada na formulação (4).

$$\begin{pmatrix} x_1 & x_2 & \cdots & x_r \end{pmatrix} = \begin{pmatrix} F_1^1 & F_1^2 & \cdots & F_1^r \\ F_2^1 & F_2^2 & \cdots & F_2^r \\ \vdots & \vdots & \ddots & \vdots \\ F_l^1 & F_l^2 & \cdots & F_l^r \end{pmatrix} \quad (4)$$

IV. Reconciliação utilizando códigos LDPC no sentido Slepian-Wolf

Após quantização dos valores das realizações de variáveis aleatórias gaussianas correlacionadas de Alice e Bob obtidas através da comunicação pelo canal quântico, estes possuem sequências binárias discretas i.i.d. representadas por $(X^{(c)})^r = [x_1^{(c)}, x_2^{(c)}, \cdots, x_r^{(c)}]$ e $(Y^{(c)})^r = [y_1^{(c)}, y_2^{(c)}, \cdots, y_r^{(c)}]$, respectivamente, para cada canal c em que $1 \leq c \leq l$, em que os pares de componentes (x_i, y_i) têm função de massa de probabilidade $p(x, y)$. As duas sequências possuídas pelas duas partes legítimas, para cada canal, portanto, devem ser decodificadas conjuntamente em um receptor comum (Bob, no caso de reconciliação direta, ou Alice, no caso de reconciliação reversa).

É assumido, para este trabalho, um processo de reconciliação direta, em vista disso, a codificação é feita no sentido de comprimir a sequência de Alice com o intuito de restringir ao máximo a informação vazada para Eva através do processo de reconciliação, já que o canal clássico é assumido perfeito. Slepian e Wolf mostraram que a região de taxas alcançáveis para esse problema, para recuperação perfeita das duas sequências em um receptor comum, é aquela identificada por

$$R_1 \geq H(X|Y) \quad (5)$$

$$R_2 \geq H(Y|X) \quad (6)$$

$$R_1 + R_2 \geq H(X, Y) \quad (7)$$

onde $H(X|Y)$ é a entropia condicional da fonte X dado a fonte Y, $H(Y|X)$ é a entropia condicional da fonte Y dado a fonte X e $H(X, Y)$ é a entropia conjunta. A região descrita pelo teorema de Slepian-Wolf é ilustrada na figura 1.

Codificando independentemente a sequência $(X^{(c)})^r$ de Alice com um codificador de fonte que conhece a correlação média entre as fontes X e Y, e assumindo que a sequência $(Y^{(c)})^r$ é comprimida para sua entropia de fonte $H(Y)$ e é conhecida pelo decodificador como informação lateral, o objetivo é comprimir a sequência $(X^{(c)})^r$ com uma taxa R_X o mais próxima possível da entropia condicional $R_X \geq H(X|Y)$ alcançando o ponto A na figura 1 [7].

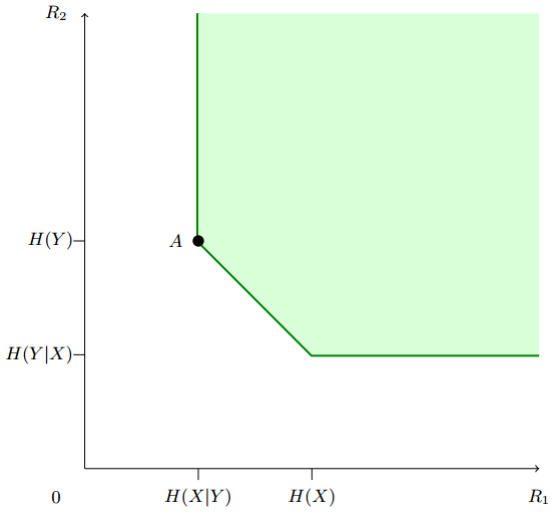

Fig. 1. Taxas para codificação Slepian-Wolf.

O decodificador deve descomprimir a sequência $(X^{(c)})^r$, para obter uma estimativa $\hat{X}$, através do emprego de $(Y^{(c)})^r$ como informação lateral. Nenhuma informação acerca da taxa é passada ao decodificador, entretanto, este conhece a correlação média de forma implícita a partir do comprimento de bloco da sequência codificada, uma vez que Alice utiliza uma taxa tão próxima quanto possível de $H(p)$, conforme mostrado no apendice I.

A. Codificação

Dada a matriz teste de paridade $H_{(n-k)\times n}$ de um código LDPC, a codificação de uma sequência binária $x^{(c)}$ gerada por Alice é feita a partir do produto $H \cdot {x^{(c)}}^T$ que corresponde à síndrome de $x^{(c)}$, Z, de tamanho $n - k$.

B. Decodificação

A decodificação foi realizada tal qual exposto em [13], de modo que a única diferença para o *Belief Propagation* tradicional é a inclusão do fator $(1 - 2s_j)$, em que s_j corresponde à j-ésima componente da síndrome, no cálculo das razões de verossimilhança enviadas pelos nós de paridade para considerar a informação recebida de Alice através do canal clássico.

V. Resultados e discussões

Conforme trazido na literatura, o protocolo SEC utiliza de 4 a 5 funções de fatiamento para realizar a reconciliação das sequências de interesse [4], [15]. Com base nesse parâmetro, o esquema proposto de quantização foi implementado no MATLAB considerando-se um total de 6 canais e um total de 20.000 a 30.000 realizações das variáveis aleatórias gaussianas correlacionadas. A probabilidade de erro e capacidade de cada canal são mostradas nas figuras 2 e 3, respectivamente.

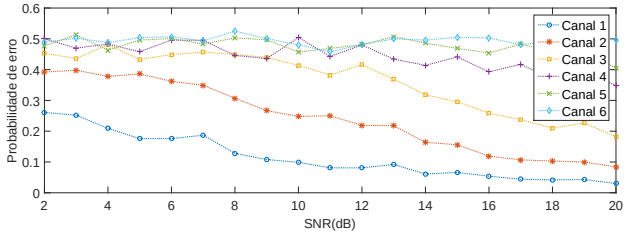

Fig. 2. Probabilidade de erro para cada canal.

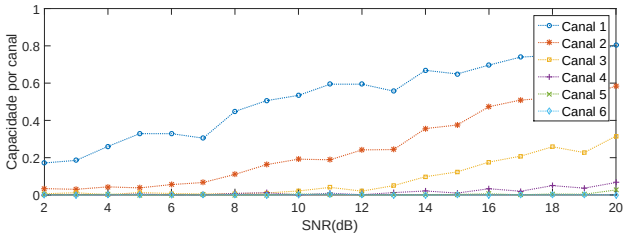

Fig. 3. Capacidade de cada canal.

Os canais de 3 a 6 se mostraram bastante ruidosos para baixos valores de SNR, não servindo para fins de compartilhamento de chaves por levarem a elevadas probabilidades de erro entre as sequências quantizadas. Entretanto, a capacidade dos canais 1 e 2 permaneceu acima do limiar 0,02 apresentado em [4], abaixo do qual considera-se, para o protocolo SEC, ser mais vantajoso revelar completamente os *bits* do que projetar bons códigos LDPC para tais taxas, já que esta deve ser menor que a capacidade do canal. Desse modo, é possível obter as mesmas taxas de chave secreta em comparação com o protocolo SEC, que para valores de SNR abaixo de 5 dB permite codificação também de apenas dois *bits* das 5 funções de fatiamento [4].

Assim, os canais 1 e 2 podem ser usados para compartilhamento da chave secreta e a estes foi aplicado o processo de reconciliação a partir da codificação/decodificação LDPC considerando as sequências binárias de Alice e Bob como realizações de fontes correlacionadas. Utilizando códigos LDPC de comprimento de bloco $N = 24576$, $N = 32000$ e $N = 32768$ com taxas $R = 2/3$, $R = 0.93$ e $R = 1/2$, respectivamente, obtiveram-se os gráficos mostrados em 4 e 5, para os quais pode-se observar que Bob corrige sua sequência a partir, unicamente, dos *bits* de paridade enviados por Alice e da sua própria sequência obtida na transmissão quântica em menos de 40 iterações, conforme observado também para o protocolo SEC em [12] para o esquema de decodificação suave que requer 35 iterações para reconciliação.

Um comparativo entre o esquema proposto de reconciliação e diferentes implementações do SEC na literatura em [4], [**?**] e [12] é apresentado na tabela V.

Uma vez que alta eficiência de reconciliação é alcançável

	Comprimento (N)	Taxas	SNR
Bloch	200.000	0/0/0,25/0,86	4,7
Guo	200.000	0/0/0,3/0,95	4,9
Li	10.000	0/0/0,3/0,9	4,5
Nosso esquema	24.576	0,66/0,95/0/0	4,5

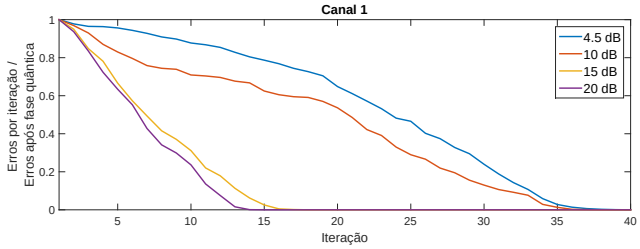

Fig. 4. Correção de erros para o canal 1 utilizando código LDPC com $N = 24576$ e $N = 32768$ e taxas $2/3$ e $1/2$, respectivamente.

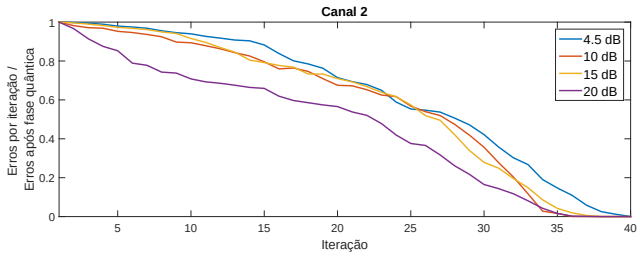

Fig. 5. Correção de erros para o canal 2 utilizando código LDPC com $N = 32000$, $N = 24576$ e $N = 32768$ e taxas 0.93, $2/3$ e $1/2$, respectivamente.

para blocos de grandes comprimentos e códigos construídos aleatoriamente, conforme mostrado em [14] e [2], trabalhos futuros incluem a construção de códigos LDPC de construção aleatória (RC – *Random Construction*) ainda na ordem de $N = 10^5$, que permitam decodificação para qualquer nível de SNR respeitadas as taxas mínimas de compressão.

VI. Considerações Finais

Neste artigo é apresentado um novo método de discretização das variáveis aleatórias gaussianas compartilhadas por Alice e Bob após a fase quântica, apresentando capacidade de gerar iguais taxas de chave secreta quando comparado com o protocolo SEC, extremamente iterativo. Os resultados exibidos para correção de erros entre as sequências binárias é objeto de estudo de trabalhos futuros, visando utilizar comprimentos de blocos assintoticamente grandes para minimizar a BER até para baixos valores de SNR.

Agradecimentos

Agradecimento à Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) pelo apoio financeiro e ao IQuanta da Universidade Federal de Campina Grande pela oportunidade de realizar esta pesquisa.

Referências

[1] ASSCHE, G. V.; CARDINAL, J.; CERF, N. J. Reconciliation of a quantum-distributed gaussian key. IEEE Transactions on Information Theory, IEEE, v. 50, p. 394 - 400, Fevereiro 2004.

[2] BAI, Z. et al. High-efficiency reconciliation for continuous variable quantum key distribution. Japanese Journal of Applied Physics 56, 044401 (2017), CrossMark, v. 56, p. 044401/1?5, Março 2017.

[3] BENNETT, C. H.; BRASSARD., G. Quantum cryptography: Public key distribution and coin tossing. Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, IEEE Press., p. 175-179, Dezembro 1984.

[4] BLOCH, M. et al. LDPC-based gaussian key reconciliation. Information Theory Workshop, IEEE, p. 116-120, Junho 2006.

[5] CHRISTIAN, K.; PIVK, M. Applied Quantum Criptography, Lecture Notes in Physics 797. 1. ed. [S.l.]: Springer, 2010. An optional note. ISBN 9783642048296.
[6] COVER, T. M.; THOMAS, J. A. Elements of Information Theory (Wiley Series in Telecommunications and Signal Processing). [S.l.]: Wiley-Interscience, 2006. ISBN 0471241954.
[7] DANESHGARAN F., LADDOMADA M. e MONDIN M., "LDPC-Based Iterative Algorithm for Compression of Correlated Sources at Rates Approaching the Slepian-Wolf Bound", Advances in Satellite and Space Communications, 2009. SPACOMM 2009. DOI: 10.1109/SPACOMM.2009.14
[8] FOSSIER, S. et al. Field test of a continuous-variable quantum key distribution prototype. New Journal of Physics 11 (2009) 045023, IOP Publishing Ltd and Deutsche Physikalische Gesellschaft, v. 11, p. 045023/1-15, Abril 2009.
[9] GROSSHANS, F.; GRANGIER, P. Continuous variable quantum cryptography using coherent states. Physical Review Lett. 88, 057902 (2002), IEEE Press., p. 1-5, 2002.
[10] JOUGUET, P.; ELKOUSS, D.; KUNZ-JACQUES, S. High bit rate continuous-variable quantum key distribution. Physical Review A 90, 042329 (2014), IEEE Press., p. 1-9, Setembro 2014.
[11] JOUGUET, P.; KUNZ-JACQUES, S.; LEVERRIER, A. Long-distance continuous-variable quantum key distribution with a gaussian modulation. Physical Review A 84, 062317 (2011), American Physical Society, p. 1-7, Dezembro 2011.
[12] LI, Q.; ZHU, R.; WANG, Y.; HAN, Q. An Improved LDPC-based SEC Error Reconciliation Scheme. 2016 Sixth International Conference on Instrumentation & Measurement, Computer, Communication and Control (IMCCC). Julho 2016. DOI:10.1109/IMCCC.2016.181
[13] LIVERIS, A. D., XIONG Z. e GEORGHIADES C. N., "Compression of Binary Sources with Side Information Using Low-Density Parity-Check Codes", Proc. of IEEE GLOBECOM 2002, vol. 2, pp.1300-1304, 17-21 Nov. 2002.
[14] LODEWYCK, J. et al. Quantum key distribution over 25 km with an all-fiber continuous variable system. Physical Review A 76, 042305 (2007), IEEE Press., v. 76, p. 042305/1-10, Outubro 2007.
[15] NASCIMENTO, E. J. do. Mapas de Shannon-Kotel'nikov na distribuição quântica de Chaves com Variáveis Contínuas. Tese (Doutorado). Universidade Federal de Campina Grande, 2017.
[16] NIELSEN, M. A.; CHUANG, I. L. Quantum Computation and Quantum Information. 10. ed. [S.l.]: Cambridge University Press, 2010. An optional note. ISBN 9781107002173.
[17] RICHARDSON, T. J.; URBANKE, R. L. Efficient encoding of low-density parity-check codes. IEEE Transactions on Information Theory, IEEE, v. 47, p. 638-656, Fevereiro 2001.
[18] RICHARDSON, T. J.; URBANKE, R. L. Modern Coding Theory. [S.l.]: Cambridge University Press 2008, 2008. ISBN 9780521852296.

APÊNDICE I
TAXA DE COMPRESSÃO DA FONTE DE ALICE

Como a sequência Y está disponível sem erros no decodificador ($R_Y = 1$), o limite teórico para compressão de X é $R_X \geq H(X|Y) = H(p)$, em que $p = P(x_j \neq y_j),\ \forall j = 1, \cdots, k$:

$$\begin{aligned} H(X,Y) &= -2\frac{p}{2}\log\frac{p}{2} - 2\frac{1-p}{2}\log\frac{1-p}{2} \\ &= H(p) + 1 \end{aligned} \tag{8}$$

Como a taxa para codificar a fonte X deve ser $R_X \geq H(X|Y)$, tem-se

$$\begin{aligned} R_X &\geq H(X,Y) - H(Y) \\ &= H(p) \end{aligned} \tag{9}$$