Fundamentos da Distribuição Quântica de Chaves

Elloá B. Guedes[1,2], Cheyenne R. Guedes Isidro[2], Bernardo Lula Jr.[2,3], Joseana Macêdo Fechine[3,4]
{elloa,cha,lula,joseana}@dsc.ufcg.edu.br

[1] Integrante do Grupo PET Computação da UFCG
[2] IQuanta - Instituto de Estudos em Computação e Informação Quânticas
[3] DSC - Departamento de Sistemas e Computação - UFCG
[4] Tutora do Grupo PET Computação da UFCG

Palavras-chave: *Distribuição quântica de chaves, criptografia, segurança*

1 Introdução

Criptografia é a ciência que estuda a troca de mensagens inteligíveis apenas aos participantes de uma dada comunicação [Burnett and Paine 2001]. A segurança da criptografia clássica possui como base um problema da complexidade computacional: dada uma função f, a partir de x é "simples"obter f(x), porém, dado um valor de f(x) é "difícil"obter o valor de x original. No escopo da criptografia, podemos traduzir essa dificuldade na intratabilidade do problema da fatoração de números primos muito grandes por computadores convencionais [Gisin et al. 2007].

Com o advento da Computação Quântica, novos algoritmos foram propostos utilizando características quânticas para tentar tornar mais eficiente a resolução de certos problemas computacionais. Dentre eles, o algoritmo de Shor reduziu o problema da fatoração ao cálculo de ordem e resolveu este problema em tempo polinomial [Shor 1994], fazendo com que se tornasse fácil quebrar a segurança dos sistemas criptográficos atuais. Dessa forma, é necessário propor novos padrões para a criptografia, em particular, no que se refere à segurança da chave criptográfica.

Este trabalho visa apresentar três padrões criptográficos relativos à distribuição quântica de chaves que propõem soluções para o problema observado.

2 Material e Metodologia

Este trabalho trata-se de um estudo teórico focado na análise dos padrões BB84, E91 e B92 para a distribuição quântica de chaves.

A distribuição de chaves é uma forma de fazer com que dois parceiros em uma comunicação criem suas chaves criptográficas. Caso seja possível realizar a distribuição de chaves de uma maneira segura então a criptografia passa a ser realizada com a utilização de uma chave simétrica [Imre and Balazs 2005]. Se esta chave criptográfica é utilizada uma única vez e é mantida em segredo pelos participantes da comunicação, então o sistema criptográfico é efetivamente seguro [Vernam 1926]. Essa é a única técnica conhecida para um sistema criptográfico totalmente seguro.

A distribuição quântica de chaves tira proveito de propriedades quânticas na tentativa de estabelecer o cenário ideal para a troca de chaves. De forma simplificada, podemos listar tais propriedades:

1. Toda medição perturba o sistema [Gisin et al. 2007];
2. Não é possível determinar com 100% de certeza a posição e o momento de uma dada partícula (Princípio da incerteza de Heisenberg) [Heisenberg 1927];
3. Não é possível medir a polarização de um fóton simultaneamente na base diagonal e retilinear (Teorema da Não-Clonagem) [Wooters and Zurek 1982];

2.1 BB84

Em 1984 foi proposto o primeiro padrão criptográfico para a troca de chaves que leva em conta as propriedades citadas anteriormente [Willians and Clearwater 1998]. O BB84 tira proveito de forma mais intensa do Teorema da Não-Clonagem e da impossibilidade de medição sem perturbação no sistema [Bennett and Brassard 1984].

No BB84, o emissor (denominado "Alice") tenta enviar uma mensagem ao destinatário (denominado "Bob"). O primeiro passo consiste em Alice efetuar o envio de uma série de qubits (bits quânticos) randômicos para Bob, ou seja, codificando-os segundo uma base retilínea ou uma base diagonal, na ordem desejada por ela. Bob, ao receber tais qubits, utiliza um beam-splitter e com ele, pode medir corretamente apenas fótons de uma destas bases. Em seguida, Bob divulga publicamente as suas escolhas de base e Alice diz quais destas escolhas foram iguais as suas. Ambos deverão considerar apenas as medições das bases em comum, ignorando o resto. O resultado da medição dessas bases pode então ser utilizado como uma chave criptográfica segura (se utilizada uma única vez e mantida em segredo), associada a algum método de criptografia clássica de chave simétrica [Mullins 2002]. É interessante notar que existem dois canais de comunicação, um quântico, no qual são trocados os fótons; e um clássico, por onde são divulgadas as escolhas de base e também onde a mensagem criptografada é enviada [Isidro and Jr. 2003]. Na figura 1 é ilustrado um cenário para obtenção de chave utilizando o BB84.

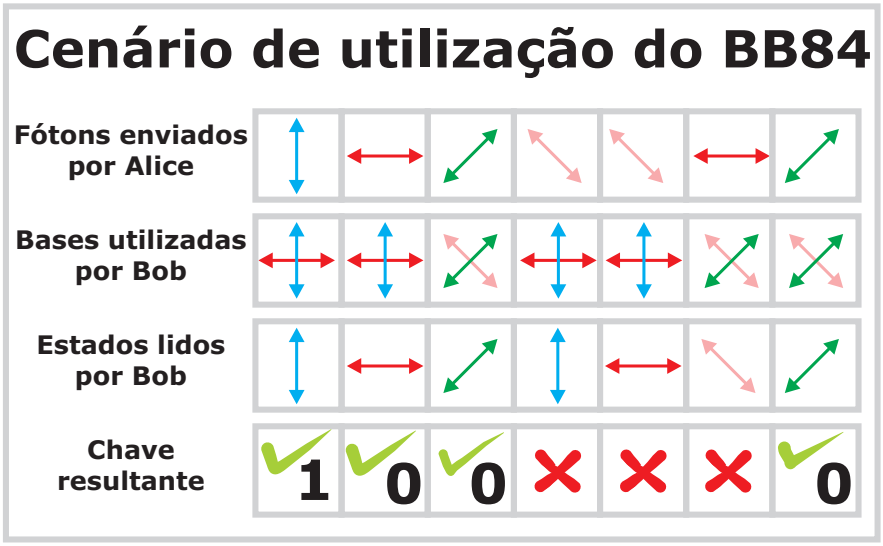

Figura 1. *Cenário de utilização do BB84*

2.2 E91

Ekert, em 1991, propôs um esquema baseado em uma propriedade de pares de sistemas quânticos correlatos, conhecida como emaranhamento. Quando um par de partículas é criado, tais partículas comportam-se como um único sistema quântico. Quando posteriormente as partículas se separam, a influência de um membro do par no outro ainda persiste. [Einstein et al. 1935].

Este procedimento para troca de chaves consiste em substituir o canal quântico carregando bits de Alice para Bob proposto no BB84 por um canal quântico carregando dois qubits de uma mesma fonte, um destinando-se a Alice e outro a Bob. A primeira possibilidade seria de a fonte emitir dois qubits no mesmo estado, originários das quatro opções possíveis a partir da utilização de bases retilíneas e diagonais, com as quais Alice e Bob mediriam os qubits. Em seguida, a fonte anuncia as suas escolhas de base e Alice e Bob mantém informações das medições efetuadas quando as bases foram compatíveis com as anunciadas [Gisin et al. 2007].

Caso a fonte seja confiável, o protocolo é equivalente ao BB84: Tudo ocorre como se o qubit fosse propagado de Alice em direção à fonte e em seguida redirecionado para Bob (contrário à linha do tempo convencional). Alice anuncia publicamente quais as escolhas de bases e Bob revela quais escolhas foram iguais, ambos utilizam

o resultado dessas medições em comum como chave criptográfica [Willians and Clearwater 1998]. Na figura 2 é ilustrado um cenário de envio das partículas simultaneamente pela fonte e a representação dos efeitos do Paradoxo de Einstein-Podolsky-Rossen no comportamento das mesmas, levando em conta as informações lidas por Alice e Bob.

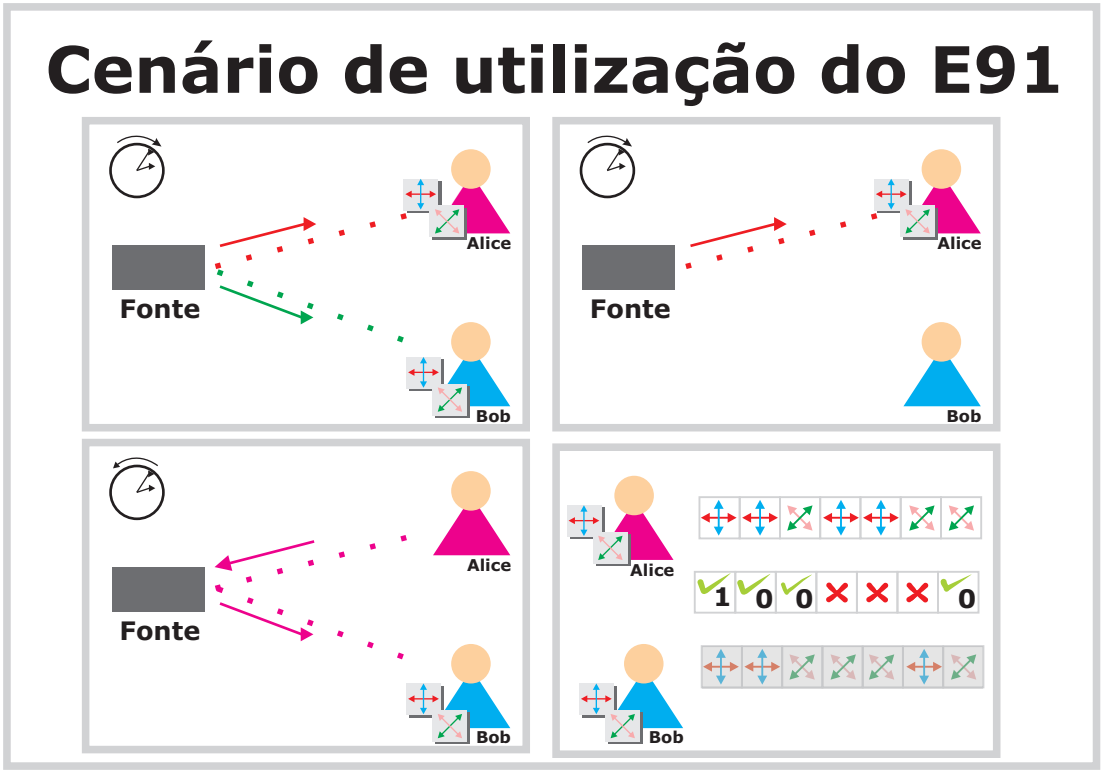

Figura 2. *Cenário de utilização do E91*

2.3 B92

Em 1992, Charles H. Bennett constatou que os quatro estados utilizados pelos padrões de distribuição de chaves quânticas propostos por padrões anteriores são excessivos para o procedimento da troca de chaves: o que importa é que existam dois estados não-ortogonais. A segurança reside na impossibilidade de um espião distinguir de forma não-ambígua e sem perturbar o sistema os estados diferentes que Alice pode enviar para Bob, supondo que dois estados são necessários e que eles são incompatíveis, então apenas eles são suficientes. [Bennett 1992].

Embora dois estados não-ortogonais não possam ser distinguidos de forma não ambígua sem perturbação, é possível realizar este procedimento com alguma perda. Assim, Alice e Bob terão que monitorar alterações do canal quântico [Gisin et al. 2007]. É também fácil perceber que diferentemente do BB84, este método pode ser realizado bit a bit [Imre and Balazs 2005].

3 Resultados e Discussões

Os padrões apresentados propõem a utilização da Mecânica Quântica para troca de chaves a fim de constituir um sistema para a troca de mensagens criptografadas totalmente seguro. As chaves obtidas são chaves seguras e podem ser utilizadas em algoritmos convencionais de chave simétrica, a exemplo do Data Encryption Standard (DES) e do Triple DES [Burnett and Paine 2001].

Para que a distribuição quântica de chaves possa ser efetuada são necessários dois canais: um canal quântico, onde serão trocados os fótons a fim de construir, a partir dos protocolos apresentados, uma chave para os participantes

da comunicação; e um canal clássico, onde a mensagem criptografada (segundo algum protocolo de criptografia de chave simétrica clássico que utiliza a chave obtida) será trocada entre os participantes [Isidro and Jr. 2003].

4 Conclusão

Este trabalho visou apresentar os três principais protocolos para a distribuição quântica de chaves. Como o objetivo deste trabalho foi apresentar de forma didática estes protocolos, não houve abordagem a cerca da implementação física dos mesmos (tecnologias utilizadas, códigos de correção de erros, etc.) e também não foi analisada a segurança destes mediante a presença de um espião na comunicação. Ainda assim, a relevância deste trabalho persiste, pois são poucas as fontes que mostram de forma esclarecedora e minimalista tais padrões.

O presente trabalho foi desenvolvido em parceria com o IQuanta - Instituto de Estudos em Computação e Informação Quânticas, localizado na Universidade Federal de Campina Grande.

Referências

[Bennett and Brassard 1984] Bennett, C. and Brassard, G. (1984). Quantum cryptography: public key distribution and coin tossing. *Int. conf. Computers, Systems & Signal Processing, Bangalore, India*, 1:175–179.

[Bennett 1992] Bennett, C. H. (1992). Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.*, 68:3121–3124.

[Burnett and Paine 2001] Burnett, S. and Paine, S. (2001). *RSA Security's Official Guide to Cryptography*. RSA Press.

[Einstein et al. 1935] Einstein, A., Podolsky, B., and Rosen, N. (1935). Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev*, 47:777–780.

[Gisin et al. 2007] Gisin, N., Ribordy, G., Tittel, W., and Zbinden, H. (2007). Quantum cryptography. *Reviews of Modern Physics*, 1.

[Heisenberg 1927] Heisenberg, W. (1927). Uber den anschaulichen inhalt der quantentheoretischen kinematik und mechanik. *Physik*, 43:172–198.

[Imre and Balazs 2005] Imre, S. and Balazs, F. (2005). *Quantum Computing and Communications - An Engineering Approach*. John Wiley & Sons, Ltd.

[Isidro and Jr. 2003] Isidro, C. R. G. and Jr., B. L. (2003). Introdução à criptografia clássica e quântica. Technical report, Departamento de Sistemas e Computação - Universidade Federal de Campina Grande.

[Mullins 2002] Mullins, J. (2002). Making unbreakable code. *IEEE Spectrum*, 1:40–45.

[Shor 1994] Shor, P. (1994). Algoritms for quantum computation: discrete logarithms and factoring. *Proceedings of the 35th Symposium on Foundations of Computer Science, Los Alamitos*, 1:124–134.

[Vernam 1926] Vernam, G. (1926). Cipher printing telegraph systems for secret wire and radio telegraphic communications. *J. Am. Institute of Electrical Engineers*, XLV:109–115.

[Willians and Clearwater 1998] Willians, C. P. and Clearwater, S. H. (1998). *Explorations in Quantum Computing*. The Eletronic Library of Science.

[Wooters and Zurek 1982] Wooters, W. and Zurek, W. (1982). A single quantum cannot be cloned. *Nature*, 299:982 – 983.