Aspectos Físicos, Matemáticos e Computacionais da Distribuição Quântica de Chaves: Protocolo BB84.

Thiago Andrade de Toledo
Instituto de Física, UFMT.
78055-000, Cuiabá, MT.
E-mail: thiagotoledo21@gmail.com

Fabrício Moraes Almeida
Instituto de Física, UFMT.
78055-000, Cuiabá, MT.
E-mail: prof.fabricio@gmail.com

RESUMO

A criptologia é uma ciência composta por duas áreas: a criptografia e a criptoanálise. A criptografia é a ciência que utiliza da matemática para cifrar e decifra uma informação, enquanto que a criptoanálise é a ciência que analisa e quebra a informação segura. Nas últimas décadas, a criptografia vem evoluindo devido ao desenvolvimento tecnológico, seja na criação de novas ferramentas ou no aprimoramento das existentes, propiciando maior segurança e privacidade para os usuários que utilizam estes mecanismos. A distribuição de chave quântica surge como forma de garantir que o monitoramento não autorizado de uma informação seja impossível, pois está baseada nas leis da Mecânica Quântica. A segurança do sistema está na impossibilidade de clonar os estados quânticos. O protocolo BB84 foi criado por Bennett e Brassard [1-2], daí o seu nome. Ele serve para troca segura de chaves quânticas e permite que dois usuários gerem uma chave secreta comum, sem a necessidade de um canal secreto previamente estabelecido [3]. Este protocolo utiliza dois níveis, os estados $|0\rangle$ e $|1\rangle$ que representam fótons linearmente polarizados em direções ortogonais. Os dois usuários devem combinar previamente os estados ortogonais de cada uma das bases que representam o bit 0 e o bit 1. Isso pode ser feito através de um canal clássico. Na notação de Dirac [4-5], o vetor de estado de um qbit, bit quântico, pode ser descrito em espaço bidimensional: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \Leftrightarrow \langle\psi| = \langle 0|\alpha^* + \langle 1|\beta^*$. E para um sistema com 2 qbits, pode-se escrever o estado deste sistema como: $|\Psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$. Dessa forma, o presente trabalho tem como objetivo demonstrar os aspectos físicos, matemáticos e computacionais da distribuição quântica de chaves com foco no protocolo BB84.

Palavras-chave: *Física. Matemática. Computação. Distribuição Quântica de Chaves.*

Referências

[1] Brassard, Crépeau, Jozsa e Langlois Gilles Brassard, Claude Crépeau, Richard Jozsa e Denis Langlois, A Quantum Bit Commitment Scheme Provably Unbreakable by both Parties, 1993.

[2] C.H. Bennett and G. Brassard, in Proceedings of IEEE 526 Rigolin e Rieznik. International Conference on Computers Systems and Signal Processing. p. 175, Bangalore, India, 1984.

[3] JABOR NETO, Filippe Coury. DUARTE, Otto Carlos Bandeira. Criptografia Quântica para distribuição de chaves.

[4] EISBERG, Robert. RESNICK, Robert. Física Quântica. Átomos, Moléculas, Sólidos, Núcleos e Partículas. 4. ed. Editora Campus, 1986.

[5] SAKURAI, Jun John. Modern Quantum Mechanics. Revised Edition. Editora Addison-Wesley, 1994.