Proceeding Series of the Brazilian Society of Computational and Applied Mathematics, v. 10, n. 1, 2023.

Trabalho apresentado no XLII CNMAC, Universidade Federal de Mato Grosso do Sul - Bonito - MS, 2023

Proceeding Series of the Brazilian Society of Computational and Applied Mathematics

Segurança Criptográfica: Combinando Métodos Clássicos e Quânticos

João Lucas Duim[1], Rafael Gomes Portácio[2]
EMAp/FGV, Rio de Janeiro, RJ

Introdução

A Criptografia Quântica é uma nova técnica da criptografia que usa os princípios da mecânica quântica para garantir a segurança de um meio comunicativo. Ela permite que não haja a necessidade de comunicação secreta prévia usada para criptografar ou descriptografar o código, tal como a chave secreta do RSA, pois nela será possível enviar uma nova chave para cada mensagem, impedindo, assim, que um agente externo consiga quebrar toda a segurança caso consiga, com algum algoritmo, descobrir a chave secreta. A criptografia quântica permite detectar se algum invasor teve acesso à informação para assim poder impedir a comunicação e é segura mesmo que o invasor tenha poder de computação ilimitado. O objetivo do presente trabalho é apresentar resumidamente duas ferramentas que, quando combinadas, permitem a troca de mensagens com criptografia teoricamente inviolável (demonstrado em [1]), o que é desejado para garantir a manutenção da segurança digital, dadas as crescentes vulnerabilidades da criptografia clássica frente aos computadores quânticos.

O Cifrador de Vernam

A tabela ASCII possui 255 caracteres, que podem ser convertidos em 8 bits binários. Seja então uma mensagem p, representada por uma sequencia de dígitos binários. Podemos criptografá-la com uma chave binária aleatória k, tal que k tenha a mesma quantidade de bits que a mensagem p. A mensagem cifrada, c, é dada por $c = p \otimes k$ onde $\otimes$ representa soma módulo 2. Isto é equivalente a fazer a porta lógica XOR bit a bit entre a mensagem e a chave. Esse sistema criptográfico chama-se Cifrador de Vernam, possui segurança perfeita (a definição rigorosa e demonstração serão omitidas nesse resumo, mas podem ser encontradas em [1]) e pode ser implementado da seguinte forma em Python:

```
def cifrador_vernam(p, k):
    c = []
    for i in range(len(p)):
         c.append((p[i]+ k[i])%2)
    return c
```

As desvantagens desse método são usar uma chave do mesmo tamanho que a mensagem original e utilizar uma nova chave aleatória para cada mensagem, pois se houver um padrão de repetição na

[1]jlduim@gmail.com
[2]rafaelportacio19@gmail.com

© 2023 SBMAC

chave, perderemos parte da aleatoriedade e abre-se margem para que mensagens sejam quebradas. O protocolo BB84, que veremos mais adiante (e que é muito bem apresentado em [2] e [3]), permite a troca segura de quaisquer chaves criptográficas e, combinado com o cifrador de Vernam, obtêm-se uma criptografia absolutamente livre de espionagem, o que não é possível classicamente.

O Protocolo BB84

Segundo o Teorema de Não Clonagem, não é possível replicar a informação quântica e nem mesmo obter informação adicional de um estado quântico genérico sem causar uma alteração no próprio estado. Segundo o Princípio da Incerteza de Heisenberg, existe um limite na precisão com que é possível medir certas grandezas do estado quântico, como momento e posição. Devido a isso, há uma série de propriedades na mecânica quântica que impõem restrições à observação e manipulação do experimento, devido a essa altíssima sensibilidade e incapacidade de medição. A Criptografia Quântica consiste justamente na utilização destas propriedades. O protocolo BB84 pode ser dividido em algumas etapas. Seja R o remetente e D o destinatário:

Passo 1 - Criação das Chaves: R envia através de fótons uma sequência de bits aleatórios para D. Dependendo do ângulo do plano da onda de luz, os fótons poderão estar em dois tipos de polarização: retilínea ou diagonal. Associam-se valores lógicos aos fótons polarizados. Por exemplo, pode-se convencionar como zero os fótons polarizados em 0 ou 45 graus, e como 1 os polarizados em 90 ou 135 graus. Para medir o fóton, D escolhe uma base aleatoriamente, mas ele só poderá obter a mesma sequência de bits de R se escolher a mesma base que ele. Se ele utilizar a base errada, o resultado obtido será outra sequência aleatória. Probabilisticamente, é esperado que as chave de R e D sejam inicialmente diferentes, devido às medições incorretas, sendo naturalmente esperado que 25% dos bits estejam incorretos, pois é esperado que metade da sequência esteja correta e a outra metade seja aleatória e acertemos apenas metade dessa metade, totalizando 75% da sequência correta.

Passo 2 - Conciliação das Bases: D divulga sua base escolhida, sem revelar o resultado obtido. R revela para D qual foi o polarizador utilizado em cada fóton, mas não qual o qubit enviado. D e R mantêm os bits cujas bases corresponderam, e formam uma chave com eles. Os caracteres da mensagem são enviados nessas posições específicas, reduzindo a chave inicial pela metade.

Passo 3 - Detectando Invasores: Para verificar se houve interceptação da comunicação, quando eles divulgam um subconjunto aleatório da chave e comparam, há um valor esperado para a taxa de erro, também chamada de QBER (quantum bit error rate). Devido aos princípios da mecânica quântica, qualquer tentativa do invasor em acessar a informação causará uma alteração no valor esperado dessa taxa. Assim, se for constatado que alguém tentou espionar a chave, ambos remetente e destinatário reiniciam o processo para não deixar a informação vazar. Caso contrário, eles removem de suas chaves os bits utilizados na verificação, e podem continuar o envio.

A simulação em Python do Protocolo BB84 será omitida nesse resumo.

Referências

[1] F. L. Marquezino e J. A. Helayël-Neto. **Estudo Introdutório do Protocolo Quântico BB84 para Troca Segura de Chaves**. Acessado em 30/03/2023, `http://qubit.lncc.br`.

[2] C. H. Bennett e G. Brassard. **Proceedings of IEEE International Conference on Computers Systems and Signal Processing**. Bangalore, Índia, 1984.

[3] G. Rigolin e A. A. Rieznik. **Introdução à criptografia quântica**. Acessado em 30/03/2023, `https://www.scielo.br`.

© 2023 SBMAC