COMPUTADORES CLÁSSICOS E QUÂNTICOS:

ESTUDOS, IMPLEMENTAÇÕES E IMPACTOS SOCIAIS

Gabriel R. Zsigmond

INICIAÇÃO CIENTÍFICA

ESCOLA SUPERIOR DE PROPAGANDA E MARKETING

Sistemas de Informação em Comunicação e Gestão

Brasil

05 de maio de 2020

Gabriel R. Zsigmond

COMPUTADORES CLÁSSICOS E QUÂNTICOS:

ESTUDOS, IMPLEMENTAÇÕES E IMPACTOS SOCIAIS

Projeto de Iniciação Científica para a Escola Superior de Propaganda e Marketing, sob a orientação do Professor Doutor Humberto Sandmann.

Orientador: Prof. Dr. Humberto Sandmann

Brasil

05 de maio de 2020

ESTUDOS, IMPLEMENTAÇÕES E IMPACTOS SOCIAIS:

ESTUDOS, IMPLEMENTAÇÕES E IMPACTOS SOCIAIS

Gabriel R. Zsigmond

Resumo

O presente projeto, ”Computadores Clássicos e Quânticos: Estudos, Implementação, Simuladores e Impactos Sociais”, se propõe a estudar a história do computador e sua evolução. A mais recente inovação na área é a computação quântica, que certamente, inaugura a próxima geração de computadores. A computação quântica muda toda uma arquitetura na forma de computação, permitindo que os novos computadores sejam exponencialmente mais eficientes quando comparados aos mais modernos da atualidade. O projeto se propõe a entender e prototipar um computador tradicional de 8 bits em hardware, usando apenas portas lógicas simples, a fim de ilustrar, de forma clara, o funcionamento de um computador tradicional. Também, esse projeto busca entender e estimar as consequências sociais que os avanços da tecnologia e o desenvolvimento da computação quântica pode gerar. Entende-se que para essa análise, se faz necessário, inicialmente, uma ampla revisão bibliográfica, a fim de comparar esses dois tipos de computadores. Para ilustrar esta, será desenvolvida uma aplicação web que simula um computador tradicional e um computador quântico executando o mesmo algoritmo. É esperado que ao final do projeto, esse estudo traga um amplo e aprofundado conhecimento da área, além de, uma contribuição em relação ao impacto social do uso computação da quântica.

Sumário

1 Introdução

1.1 Definição justificada dos objetivos e da sua relevância

A palavra “computador” é usada desde o século XVII, tendo a sua primeira referência escrita datada de 1613. No entanto, por muito tempo “computador” não tinha o mesmo significado que leva hoje, sendo utilizada, até a década de 1940, como nome da profissão de alguém que calcula, segundo o dicionário Michaelis: “Aquele ou aquilo que calcula baseado em valores digitais; calculador, calculista”. [4]

Tendo em vista o antigo significado da palavra “computador”, pode-se questionar sobre como passamos a utilizar de uma palavra usada para se referir à pessoas, para mera maquinas. A fim de responder essa pergunta, recuperaremos a origem dos computadores. Pode parecer uma pergunta simplista que não precisa ser respondida, porém, é uma pergunta para a qual muitas pessoas não sabem a verdadeira resposta. Computadores existem há muito mais tempo que o transistor – dispositivo semicondutor usado para amplificar ou alternar sinais eletrônicos e eletricidade. – na forma mecânica e teórica. A definição real de um computador foi elaborada por Alan Turing (Reino Unido, 1912-1954), um matemático, lógico, criptógrafo e herói de guerra que se preocupava exatamente com a questão relacionada ao que era computável e o que não era. Ele foi responsável por elaborar a definição do computador, descrevendo a Maquina de Turing, trabalho publicado em 1937 que deu origem aos computadores e celulares que você, leitor, pode estar usando para ler o presente trabalho.

A Maquina de Turing, considerado o modelo mais poderoso computador, é similar a um automato finito [1], porém com uma mémoria ilimitada e irrestrita, constituindo um modelo mais exato de um computador de forma geral. Esta é composta por três principais componentes: fita infinita; processador; máquina de estado finito.

A fita infinita é dividida em células, cada uma contendo um simbolo de um alfabeto

[1] Um sub-tópico da Ciência da computação teórica, também chamado máquina de estados finita determinística — é uma máquina de estados finita que aceita ou rejeita cadeias de símbolos gerando um único ramo de computação para cada cadeia de entrada.

finito. O processador é responsável por se deslocar para a direita ou esquerda e efetuar a leitura ou escrita em uma célula. Assim, a explicação adaptada do material do Prof. Dr. Fabio Gagliardi Cozman [3], ilustra seu funcionamento da seguinte forma:

1. Inicialmente a fita contém somente a cadeia de entrada, disposta no “meio” [2] da fita , com o processador posicionado no início da cadeia (o resto está em branco);

2. Para armazenar algo, a máquina escreve na fita;

3. O processador pode ser movido livremente para a esquerda ou direita, afim de ler ou escrever valores em qualquer célula;

4. As saídas aceita e rejeita são obtidas ao entrar nos estados de aceitação e rejeição;

5. Se não entrar em um estado de aceitação ou rejeição, continuará sua computação para sempre (loop infinito).

Já o primeiro computador digital eletrônico de grande escala, foi criado em fevereiro de 1946 por cientistas norte-americanos, John Presper Eckert e John W. Mauchly, da Electronic Control Company . No final de sua operação em 1956, o ENIAC (Electrical Numerical Integrator and Calculator), continha 20.000 tubos de vácuo 7.200 diodos de cristal 1.500 relés 70.000 resistores 10.000 capacitores e aproximadamente 5.000.000 juntas soldadas à mão. Ele pesava mais de 27 toneladas, tinha aproximadamente 2,4m * 0,9m * 30m de tamanho, ocupava 167 m2 e consumia 150 kW de eletricidade. [13]

A partir do ENIAC, as possibiliades tecnologicas tomaram uma nova proporção. Em 1969, apenas 13 anos após o desligamento do primeiro computador digital eletronico, o computador de bordo da Apollo 11, missão que levou o homem a lua, tinha 32.768 bits [para uma explicação elaborada sobre bits refira-se ao cápitilo 2 pagina 8] de RAM, o suficiente para armazenar apenas um texto não formatado, com cerca de

[2] Meio é algo abstrato nesse sentido pois não existe meio de um valor infinito

2.000 palavras. Em 2018, o iPhone XS, com 4GB de RAM (ou 34.359.738.368 bits), tem cerca de 1 milhão de vezes mais memória que o Apollo Guinche Computer. [9]

(falar da Spacex e falcon9 e CRS-12 Dragon 2020)

Durante o século XX, além do aumento de poder computacional dos dispositivos, outro fator impactante foi a refatoração de seus tamanhos. Assim, com tecnologias wearables [3], os computadores se tornam ativamente presentes no cotidiano.

Levando em consideração o rápido avanço e desenvolvimento computacional, mencionados anteriormente, entende-se que os computadores agregam à sociedade, seja facilitando a comunicação e o compartilhamento de conhecimentos, como em outros aspectos. No entanto, a agilidade pela qual se deu tais transformações da tecnologia da computação, também gera grandes expectativas e incertezas sobre o que ainda está por vir, tanto nas questões de mudanças tecnológicas quanto nos impactos relevantes na sociedade.

Tendo em vista a incerteza sobre o futuro da computação em relação aos proximos grandes avanços, nessa pesquisa serão estudados os conceitos da física clássica e da física quântica aplicados à computação, além disso, será estudado os princípios de criptografia [4]. Assim, a presente pesquisa irá prototipar um computador clássico de 8 bits em hardware usando apenas portas lógicas simples, dessa forma, ilustrando claramente o seu funcionamento. Junto a isso também será desenvolvida uma aplicação web que ilustre o funcionamento de um processador quântico. Ao final, conceitos de criptografia serão ultilizados para exemplificar possíveis mudanças sociais que os próximos avanços tecnologicos podem gerar.

[3] A tecnologia em questão não somente pode ser usada como uma peça de roupa ou um acessório, como também tem que possuir características que a conectem a outros aparelhos ou à internet.

[4] Criptografia é um sistema de algoritmos matemáticos que codificam dados para que só o destinatário possa ler.

1.2 Metodologia a ser empregada

Para a realização da pesquisa de iniciação científica, é indispensável o uso de pesquisa bibliográfica, assim recuperando conhecimento científico acumulado sobre o assunto. Segundo Telma Cristiane Sasso de Lima, o conhecimento da realidade não é apenas a simples transposição dessa realidade para o pensamento, pelo contrário, consiste na reflexão crítica que se dá a partir de um conhecimento acumulado e que irá gerar uma síntese, o concreto pensado [5]. E também a utilização do processo científico para a elaboração e efetivação do projeto em si. Ambas metodologias citadas acima, são cruciais para o desenvolvimento do relatório final na área de pesquisa em computação, já que na grande parte dos estudos científicos, a utilização do processo científico é frequentemente utilizada para um maior entendimento da obra e a construção do projeto se tornar mais facilmente executável.

Para o desenvolvimento da entrega do protótipo, computador de 8-bits, e para o simulador do computador quântico web, a principal metodologia utilizada será Project Based Learnig (PBL). De acordo com David Van Andel, o PBL envolve os alunos em um processo rigoroso de investigação, onde eles fazem perguntas, encontram recursos e aplicam informações para resolver problemas do mundo real [2]. Assim, assumisse que esta é a melhor metodologia para desenvolver um protótipo físico de um computador e programar um site.

2 Computação Clássica

Entende-se a importância de se compreender a origem e o desenvolvimento da computação clássica para o desenrolar da pesquisa, o que será apresentado em meio a este capítulo.

A computação clássica consiste em computadores que dependem da física clássica para operar. Estes são os computadores tradicionais que usamos em nosso dia-a-dia – seja eles Apple, Samsung, Dell ou qualquer outro –, também classificados como computadores binários, pois processam as instruções a partir de números binários, compostos apenas pelos símbolos “1” e “0”, ligado e desligado respectivamente. Assim, julga-se importante e de larga relevância ao tema compreender essa representação numérica.

Números binários ou números em base 2 são compostos por apenas dois dígitos, [0...1]. Dessa forma, seu funcionamento é similar ao sistema decimal, ou base 10, que são compostos por dez dígitos, [0...9]. No sistema decimal, é simples contar até nove, porém não existe um simbolo ou dígito para representar o número dez, sendo então representado dois dígitos, “10”. Isto é uma simples lógica de posicionamento. Mais uma vez, após o número “99”, é necessário utilizar a mesma regra para representar o número cem, “100”. Em base 2, o número zero é representado pelo simbolo 0, e o número um por 1. O mesmo dilema é enfrentado ao chegar no próximo valor, dois. E então é usada a mesma lógica de posicionamento, em base dois. O número dois é representado por “10”, o três por “11”, quatro por “100” e assim por diante. Dessa forma, números binários podem se tornar longos e compostos por muitos dígitos. Em computação, esses dígitos são chamados de bits. [7] É com base nos bits [5] ligados e desligados que o computador baseia sua linguagem. Para transforma-lo em base dez é preciso avaliar o valor de cada bit de acordo com a sua posição.

Exemplo: número binário 1011:

[5] A menor unidade de informação que pode ser armazenada ou transmitida na comunicação de dados.

$$1011(b) = 1 * 2^3 + 0 * 2^2 + 1 * 2^1 + 1 * 2^0$$

$$= 8 + 0 + 2 + 1 = 11(decimal)$$

O peso de cada bit de um número binário depende da sua posição relativa ao número completo, sempre partindo da direita para a esquerda.

- O peso do primeiro bit é $bit * 2^0$
- O peso do segundo bit é $bit * 2^1$
- O peso do terceiro bit é $bit * 2^2$
- O peso do quarto bit é $bit * 2^3$

A formúla ilustrada acima, pode ser exemplificada em uma fórmula genérica:

$$= nth\ bit * 2^{n-1}$$

É possível notar que a regra para números binários, se repete para números em base 10.

Exemplo: número decimal 4392:

- O peso do primeiro bit é $2 * 10^0$
- O peso do segundo bit é $9 * 10^1$
- O peso do terceiro bit é $3 * 10^2$
- O peso do quarto bit é $4 * 10^3$

$$4392 = 4 * 10^3 + 3 * 10^2 + 9 * 10^1 + 2 * 10^0$$

$$= nth\ bit * 10^{n-1}$$

Essa regra se mantem verdadeira para qualquer base númerica.

$$= nth\ bit * (base)^{n-1}$$

Ao decorrer do texto serão referidos números em base 2, 10 e 16.

2.1 A computação clássica e sua evolução

Alan Turing, Matemático inglês, cientista da computação, lógico, criptoanalista, filósofo e biólogo teórico, publicou o artigo “On Computable Numbers with an Application to the Entscheidungs-problem” [12] em 12 de novembro de 1937, esse formaria a teoria básica da computabilidade por várias décadas.

O mecanismo abstrato descrito no artigo de Turing fornece os conceitos fundamentais de computadores que outros engenheiros conceberam posteriormente. Na sua essência, uma Máquina de Turing é um dispositivo que manipula símbolos em uma tira de fita de acordo com uma tabela de regras. Forneceu formalização dos conceitos de “algoritmo” e “computação” na infância da ciência da computação. Apesar de sua simplicidade, uma Máquina de Turing pode ser adaptada para simular a lógica de qualquer algoritmo de computador e é útil para explicar as funções de uma CPU.

Turing é identificado não apenas como o pai da ciência da computação, mas também como o pai do computador clássico. O fundamento para isso é o seguinte, o diagrama do computador moderno pode ser encontrada no projeto EDVAC de Von Neumann [6] e hoje os computadores clássicos são geralmente descritos como tendo a chamada arquitetura de Von Neumann. Uma idéia fundamental do design do EDVAC é a idéia de programa armazenado. Isso significa o armazenamento de instruções e dados na mesma memória, permitindo a manipulação de programas como dados. Existem razões para supor que Von Neumann conhecia os principais resultados do trabalho de Turing [1]. Assim, pode-se argumentar que o conceito de programa armazenado se origina da noção de máquina de Turing e, destacando isso como a característica definidora do computador clássico, alguns podem alegar que Turing é o pai do computador até o estado da arte. Outro argumento relacionado é que Turing foi o primeiro a explorar a idéia de uma máquina de uso geral por meio de sua noção de máquina universal e que, nesse sentido, ele também “inventou” o computador moderno. Esse argumento é reforçado pelo fato de que Turing também estava envolvido na construção de uma classe importante de dispositivos de computação, o Bombe [6].

[6] um dispositivo eletromecânico usado pelos criptologistas britânicos para ajudar a decifrar as men-

Posteriormente, ele propôs o design do ACE (Automatic Computing Engine), explicitamente explicado. identificado como um tipo de realização física da máquina universal pelo próprio Turing:

"Some years ago I was researching on what might now be described as an investigation of the theoretical possibilities and limitations of digital computing machines. [. . .] Machines such as the ACE may be regarded as practical versions of this same type of machine." [11]

Baseando na teoria da máquina de Turing, o físico e matemático John von Neumann desenvolveu uma arquitetura que era capaz de executar tais tarefas.

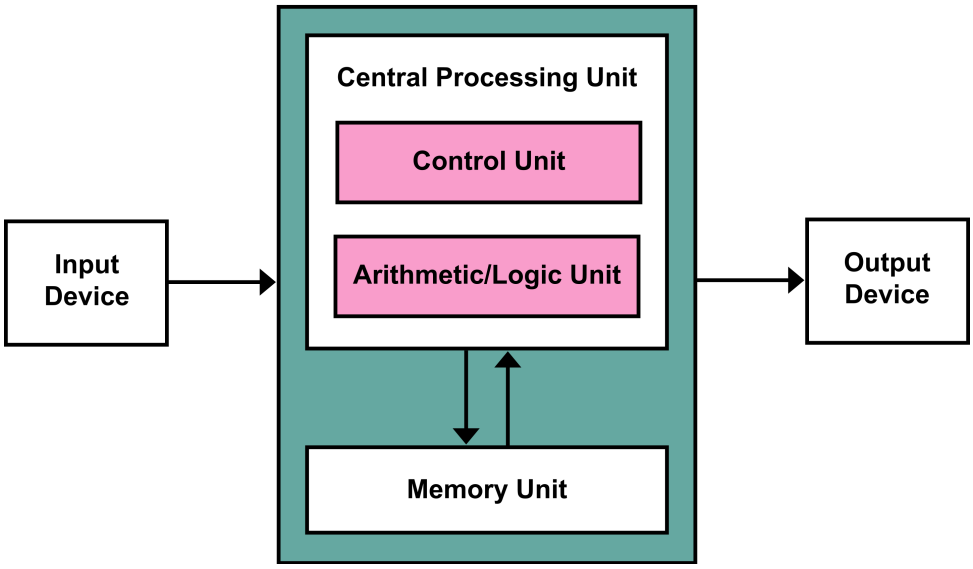

Figura 1: Diagrama arquitetura de Von Neumann

Nessa arquitetura, o cabeçalho passa a ser uma CPU (Central Processing Unit), a fita se transforma em memória RAM e as operações são construidas e executadas em circuitos formados por portas logicas chamado ALU (Arithmetic/Logic Unit). [8]

Atualmente, a maioria dos computadores modernos são construídos sobre a praxis da arquitetura von Neumann. A fim de simular um processador moderno de forma didática, foi elaborado o ASM 24bits este apresenta as principais características de

sagens secretas criptografadas pela máquina alemã Enigma durante a Segunda Guerra Mundial.

um processador moderno e permite a sua programação utilizando um Assembly de 20 instruções, sua Documentação. Similar à arquitetura de von Neumann esse emulador é composto por memória e CPU.

Registradores	
Nome	Descrição
Accumulator (ACC)	Este é o registro mais usado para armazenar dados extraídos da memória. Está em diferentes números em diferentes microprocessadores.
Instruction Register (IR)	É o registro que contém a instrução que está sendo executada atualmente.

3 Computação Quântica

3.1 A computação quântica e sua evolução

4 Computador

Construir um computador parece uma tarefa complicada e assustadora. Porém, uma CPU [7] é bastante simples em operação depois que os fundamentos por trás de todos os seus processos são compreendidos. Este capítulo destina-se a executar o passo a passo para que qualquer pessoa interessada seja capaz em construir seu próprio computador e obter o conhecimento que acompanha o processo.

4.1 Módulos

Para facilitar o compreendimento, e também o desenvolvimento do computador, este capítulo será dividido em alguns subcapitulos, assim cada um abordará uma parte do computador.

4.1.1 Clock

O clock do computador é uma parte essencial para o seu funcionamento. Este tem a função de sincronizar todas as operações. A ação mais rápida que o computador consegue executar é equivalente a uma vibração do seu clock.

4.1.2 Registers

A maioria das CPUs possuem vários registradores que armazenam pequenas quantidades de dados que a CPU está processando. Em nossa CPU de breadboard,

[7] CPU é a sigla para Central Process Unit, ou Unidade Central de Processamento. É o principal item de hardware do computador, que também é conhecido como processador, essa é a parte responsável por calcular e realizar tarefas determinadas pelo usuário.

criaremos três registradores de 8 bits: A, B e IR. Os registradores A e B são registradores de uso geral. O IR (instruction register) funciona da mesma forma, porém apenas o usamos para armazenar a instrução atual que está sendo executada.

4.1.3 Arithmetic logic unit (ALU)

A parte da unidade lógica aritmética (ALU) de uma CPU geralmente é capaz de executar várias operações aritméticas, bit a bit e de comparação em números binários. Em nossa CPU de breadboard, a ALU pode apenas adicionar e subtrair. Ele está conectado aos registros A e B e gera a soma de A + B ou a diferença de A-B.

4.1.4 Random access memory (RAM)

A memória de acesso aleatório (RAM) armazena o programa que o computador está executando, bem como todos os dados que o programa precisa. Nosso computador de breadboard utiliza endereços de 4 bits, o que significa que ele terá apenas 16 bytes de RAM, limitando o tamanho e a complexidade dos programas que ele pode executar.

4.1.5 Program counter

O contador do programa (Program counter) conta em binário para acompanhar qual instrução o computador está executando no momento.

4.1.6 Output register

O registro de saída é semelhante a qualquer outro registro (como os registros A e B), exceto que, em vez de exibir seu conteúdo em binário em 8 LEDs, ele exibe seu conteúdo em decimal em um display de 7 segmentos. Fazer isso requer alguma lógica complexa.

4.1.7 CPU control logic

A lógica de controle é o coração da CPU. É o que define os códigos de operação (opcode) que o processador reconhece e o que acontece quando ele executa cada instrução.

4.1.8 Materiais Necessários

5 Simulador

6 Criptografia

Conforme definido por Bruce Schneier *"The art and science of keeping messages secure is cryptography [...]."* [10] Embora a criptografia é considerada fundamental em nossas vidas digitais, não está especificamente relacionada à computação. Ele existe em diversas formas há milênios.

Na segurança cibernética, há uma série de coisas com as quais nos preocupamos quando se trata de dados. Isso inclui confidencialidade, integridade, disponibilidade e não repúdio.

Confidencialidade significa que nossos dados não podem ser acessados / lidos por usuários não autorizados.

Integridade significa que nossos dados chegam a nós 100% intactos e não foram modificados, seja por um ator malicioso, perda de dados ou outros.

Disponibilidade significa que nossos dados estão acessíveis quando necessário.

Não-repúdio significa que, se Bob enviar alguns dados para Mary, ele não poderá alegar mais tarde que não era, de fato, o remetente dessa informação. Em outras palavras, existe uma maneira de determinar que ninguém além de Bob poderia ter enviado os dados.

A criptografia não faz muito por nós no que diz respeito à disponibilidade, mas examinaremos as várias formas de criptografia digital e como elas podem nos ajudar a alcançar os outros três objetivos listados acima. Quando falamos de criptografia digital, geralmente nos referimos a um dos seguintes:

1. Criptografia simétrica
2. Criptografia assimétrica
3. Funções de hash
4. Assinaturas digitais

Esses conceitos serão explicados e exemplificados na próxima secção.

6.1 Conceitos básicos de criptografia

Antes de mergulharmos nisso: o que exatamente queremos dizer com ”criptografia”? Criptografar e descriptografar são normalmente usadas para significar criptografia e decifração, respectivamente; Para simplificar, criptografar uma mensagem significa torná-la ilegível para partes não autorizadas usando uma cifra (o método específico para fazer isso). Descriptografar a mensagem significa reverter o processo e tornar os dados legíveis mais uma vez.

6.1.1 Criptografia simétrica

Para criptografar e descriptografar corretamente nossos dados, precisamos dos dados e de uma chave (que determina a saída da nossa cifra). Com a criptografia simétrica, a chave usada para criptografar e descriptografar dados é a mesma.

6.1.2 Criptografia assimétrica

O problema da criptografia simétrica é o seguinte: E se eu precisar enviar dados com segurança em um ambiente hostil, como a Internet? Se a mesma chave for usada para criptografar e descriptografar dados, primeiro eu precisaria enviar a chave de descriptografia para estabelecer uma conexão segura. Mas isso significa que estou enviando a chave por uma conexão insegura, o que significa que a chave pode ser interceptada e usada por terceiros! Como contornar isso?

Para exemplificar, usaremos um cadeado que possui três estados: A (bloqueado), B (desbloqueado) e C (bloqueado). E tem duas chaves distintas. A primeiro pode girar apenas no sentido horário (de A a B a C) e a segunda pode girar apenas no sentido anti-horário (de C a B a A).

Ao criptografar uma mensagem, o usuário pega a primeira chave e guarda para si mesmo. Essa chave, sua chave ”privada- porque apenas ele a possui.

A segunda chave, sua chave “pública”: Pode ser distribuida para qualquer pessoa. Assim, o usuário tem sua chave privada que pode mudar de A para B para C. E todo os outros tem sua chave pública que pode mudar de C para B para A.

Colocando isso em pratica, imagine que você queira enviar um documento privado para o usuario. Você coloca o documento na caixa e usa uma cópia da chave pública dele para bloqueá-lo. Lembre-se de que a chave pública dele gira apenas no sentido anti-horário, e você a coloca na posição A. Agora a caixa está bloqueada. A única chave que pode passar de A para B é a chave privada, a que ele guardou para si.

6.1.3 Funções de hash

Uma função de hash, diferente da criptografia simétrica / assimétrica, é uma função unidirecional. Você pode criar um hash a partir de alguns dados, mas não há como reverter o processo. Como tal, não é uma maneira útil de armazenar dados, mas é uma maneira útil de verificar a integridade de alguns dados. Uma função de hash recebe alguns dados como entrada e gera uma string aparentemente aleatória (mas nem tanto) que sempre terá o mesmo comprimento. Uma função de hash ideal cria valores exclusivos para diferentes entradas. A mesma entrada exata sempre produzirá exatamente o mesmo hash - e é por isso que podemos usá-la para verificar a integridade dos dados.

6.1.4 Assinaturas digitais

As assinaturas digitais são ótimas tanto para integridade quanto para não repúdio. Uma assinatura digital é uma combinação de hash e criptografia assimétrica. Ou seja, uma mensagem é o primeiro hash e esse hash é criptografado com a chave privada do remetente. Isso constitui a assinatura, que é enviada junto com a mensagem. O destinatário usa a chave pública do remetente para extrair o hash da assinatura e a mensagem é hash para comparar com o hash extraído. Se você tiver certeza de que a chave pública pertence ao remetente e a descriptografia da chave pública for bem-sucedida, pode ter certeza de que a mensagem realmente veio do remetente. Se o

hash extraído corresponder ao hash computado da mensagem, você pode ter certeza da integridade da mensagem.

6.2 Criptografia aplicada computação clássica

6.3 Criptografia aplicada computação quântica

7 Próximos passos

7.1 Plano de Redação

7.2 Cronograma

7.3 Problemas

8 Impactos sociais

9 Conclusões

9.1 Perspectivas

Referências

[1] *A Half-Century Survey on The Universal Turing Machine*, USA, 1988. Oxford University Press, Inc.

[2] Grand Rapids Business Journal – David Van Andel. Project-based learning is the future of education, out. 2019.

[3] Fabio Gagliardi Cozman. Turing e complexidade. University Lecture, 2000.

[4] Melhoramentos ltda. – Michaels. Computador, out. 2019.

[5] Regina Célia Tamaso Mioto. Procedimentos metodológicos na construção do conhecimento científico: a pesquisa bibliográfica. *Revista Katálysis*, 10(SPE):37–45, 2007.

[6] John von Neumann. First draft of a report on the edvac. Technical report, 1945.

[7] B. Ram. *Computer Fundamentals: Architecture and Organization*. New Age International, 2000.

[8] Humberto Rodrigo Sandmann. Ambiente de produção. personal website, 2019.

[9] UOL – Bruno Santana. Iphone 6 é 120 milhões de vezes mais poderoso que o computador de bordo da apollo 11, jul. 2019.

[10] Bruce Schneier and Phil Sutherland. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. John Wiley and Sons, Inc., USA, 2nd edition, 1995.

[11] A. M. Turing, Michael Woodger, B. E. Carpenter, and R. W. Doran. *A. M. Turing's ACE Report of 1946 and Other Papers*. The MIT Press, Cambridge, Mass. : Los Angeles, April 1986.

[12] Alan M. Turing. On computable numbers, with an application to the Entscheidungsproblem. *Proceedings of the London Mathematical Society*, 2:230–265, 1936.

[13] Paul Wazlawick. *História da computação*. Elsevier, Rio de Janeiro, RJ, 2016.