

UNIVERSIDADE FEDERAL DO RIO DE JANEIRO
INSTITUTO DE MATEMÁTICA

GIANCARLO KLEMM CAMILO

**Análise do Sistema de Criptografia
Completamente Homomórfico de
Gentry**

Prof. Luiz Carlos Pessoa Albini, Ph.D.
Orientador

Curitiba, Dezembro de 2015

Análise do Sistema de Criptografia Completamente Homomórfico de Gentry

Giancarlo Klemm Camilo

Projeto Final de Curso submetido ao Departamento de Ciência da Computação da Universidade Federal do Paraná como parte dos requisitos necessários para obtenção do grau de Bacharel em Ciência da Computação.

Apresentado por:

Giancarlo Klemm Camilo

Aprovado por:

Prof. Luiz Carlos Pessoa Albini, Ph.D.

Prof. Nome do participante banca 1, D.Sc.

Prof. Nome do participante banca 2, Ph.D.

Prof. Nome do participante banca 3, Ph.D.

CURITIBA, PR - BRASIL

Dezembro de 2015

Agradecimentos

Agradeço à...

RESUMO

Análise do Sistema de Criptografia Completamente Homomórfico de Gentry

Giancarlo Klemm Camilo

Dezembro/2015

Orientador: Luiz Carlos Pessoa Albini, Ph.D.

Resumo...

ABSTRACT

Análise do Sistema de Criptografia Completamente Homomórfico de Gentry

Giancarlo Klemm Camilo

Dezembro/2015

Advisor: Luiz Carlos Pessoa Albini, Ph.D.

Abstract...

Lista de Abreviaturas e Siglas

RSA RSA é um sistema de criptografia de chave pública criado por Ron Rivest, Adi Shamir e Leonard Adleman

Sumário

Agradecimentos	i
Resumo	ii
Abstract	iii
Lista de Abreviaturas e Siglas	iv
1 Criptografia Completamente Homomórfica	1
1.1 Introdução	1
1.2 Criptografia completamente homomórfica	3
1.3 Aplicações	4
1.3.1 Computação em nuvem	4
1.3.2 Secure multi-party computing	5
1.3.3 Assinaturas homomórficas para network coding	5
1.3.4 Outras	6
1.3.5 Limitações atuais	6
1.4 Construção do sistema	7
1.4.1 Sistema parcialmente homomórfico	8

1.4.2	De parcialmente para completamente homomórfico	9
1.4.3	Simplificando a descriptografia	10
1.4.4	Como as operações funcionam	11
1.5	Segurança	12
1.5.1	Ataques conhecidos	12
1.6	Implementação do algoritmo	14
1.6.1	O que está implementado	14
1.6.2	Diferenças entre a implementação e o sistema de Gentry	14
1.7	Testes e Comparações	15
1.7.1	Arquitetura usada	15
1.7.2	Implementação usada para comparação	15
1.7.3	Metodologia	15
1.7.4	Resultados	16
1.8	Conclusões	17

Capítulo 1

Criptografia Completamente Homomórfica

1.1 Introdução

Esta monografia tem como objetivo apresentar o problema da Criptografia Completamente Homomórfica com suas possíveis aplicações e limitações. Essa criptografia, apesar de recente, tem a capacidade de inovar o campo de computação em nuvem, uma vez que ela torna possível a confidencialidade neste sistema. A solução apresentada por Gentry para o problema de Criptografia Completamente Homomórfica, atualmente considerado a melhor solução para tal problema, é descrita com relação a criptografia sobre inteiros e seu método de construção é explicado seguindo os passos de construção originais.

Uma seção é dedicada a verificar a segurança deste sistema de criptografia, verificando o que garante que nenhuma informação seja liberada quando operações são aplicadas ao texto criptografado uma vez que uma dica sobre a chave privada é inserida. Além disso, testes foram realizados utilizando uma implementação deste sistema de criptografia ¹ e seus resultados foram comparados com outros sistemas de criptografia conhecidos, como RSA.

¹A implementação escolhida é baseada na criptografia com relação a inteiros, que é explicada em [?]

Concluimos com algumas observações sobre as diferenças entre essa criptografia e outras criptografias assimétricas, limitações atuais, possibilidades futuras e melhorias necessárias para fazer com que a criptografia completamente homomórfica possa ser usada em larga escala.

1.2 Criptografia completamente homomórfica

Um sistema de criptografia é chamado de homomórfico quando é possível fazer operações matemáticas nos dados criptografados de modo que, quando eles forem descriptografados, as operações matemáticas foram aplicadas aos dados originais, sem que informações sobre o texto original tenham vazado. Ou seja, um número x é criptografado e uma operação de multiplicação por 2 é feita nos dados criptografados, quando os dados forem criptografados o resultado será $2 * X$.

Essa noção de criptografia foi formalmente apresentada logo após a invenção do RSA quando foi observado que ele é homomórfico em relação a multiplicação, porém não para adição. Isso levou a inevitável questão de se é possível criar um sistema que seja homomórfico com relação a adição e multiplicação (Completamente homomórfico) e o que podemos fazer com tal sistema.

Como qualquer função computacional pode ser representada por adições e multiplicações, isso significa que poderíamos executar qualquer função sem saber os dados originais. Várias aplicações seriam possíveis para um sistema como este, tais como computação em nuvem compatível com privacidade, bancos de dados privados, tercerização de processamento de modo seguro, entre outros descritos na seção seguinte.

Só depois de 30 anos após a invenção do RSA uma solução plausível foi encontrada. Ela foi apresentada por Gentry em * e sua construção é explicada em detalhes na seção *.

1.3 Aplicações

Possível aplicações para um sistema completamente homomórfico... Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

1.3.1 Computação em nuvem

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

1.3.2 Secure multi-party computing

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

1.3.3 Assinaturas homomórficas para network coding

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

1.3.4 Outras

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

1.3.5 Limitações atuais

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

1.4 Construção do sistema

O sistema apresentado por Gentry é um sistema de criptografia assimétrico com quatro algoritmos básicos: *KeyGen*, *Encrypt*, *Decrypt* e *Evaluate*. *KeyGen* gera uma chave pública (Disponível para qualquer um) e uma chave privada, o algoritmo *Encrypt* usa a chave pública para criptografar os dados e o algoritmo *Decrypt* usa a chave privada para descriptografar os dados. A diferença desse modelo para um sistema de chave pública não completamente homomórfico está no algoritmo *Evaluate*. Este algoritmo suporta certas funções que podem ser aplicadas nos dados, de modo que para cada função f o algoritmo *Evaluate* recebe um texto que criptografa os dados (m_1, m_2, \dots, m_i) e retorna um texto que criptografa $f(m_1, m_2, \dots, m_i)$.

Para que o sistema seja completamente homomórfico, o algoritmo *Evaluate* deve computar qualquer algoritmo de computador. Um modelo equivalente é a máquina de Turing, que pode simular qualquer algoritmo usando adições, subtrações e multiplicações². Logo, nosso algoritmo só precisa computar essas três funções.

Antes de começar a construção precisamos formalizar algumas restrições para o sistema de criptografia, uma vez que o objetivo desse tipo de criptografia é que 'processamento' possa ser delegado de modo seguro. A complexidade para descriptografar a saída de *Evaluate* deve ser igual a de descriptografar a saída de *Decrypt*, as saídas dessas funções devem ter o mesmo tamanho, a complexidade para descriptografar deve ser independente da complexidade das funções suportadas por *Evaluate*. Além disso a função *Evaluate* deve ser eficiente, ou seja, deve depender polinomialmente somente do tamanho da chave e da complexidade das funções suportadas (A complexidade das funções pode ser medida pelo tempo ela requiere em uma máquina de turing ou, análogamente, pelo tamanho de um circuito booleano necessário para computar a função).

Para chegar a um sistema completamente homomórfico, Gentry mostra a construção de um sistema parcialmente homomórfico, de modo que o algoritmo *Evaluate* pode computar um número limitado de funções, porém não funções muito complica-

²Multiplicações modulo 2

das. Em seguida esse sistema é estendido para que possa executar qualquer função, ou seja, ele é completamente homomórfico.

1.4.1 Sistema parcialmente homomórfico

Para um parâmetro de segurança λ , o sistema parcialmente homomórfico funciona da seguinte maneira:

- *KeyGen*(λ): A chave privada sk é um inteiro de λ^2 bits. A chave pública pk é uma lista de inteiros que são criptografias de zero³. Os textos da chave pública são criptografados como $c = sk * q + 2r$, onde q é um inteiro aleatório de λ^5 bits e $2r < sk/2$.
- *Encrypt*(pk, m): Um bit m é criptografado como $m + 2 * r + 2 * sum$, onde sum é uma soma de um conjunto de textos criptografados da chave pública, e r é um número aleatório tal que $-(2^p) < r < (2^p)$ para $p = \lambda^2$.
- *Decrypt*(sk, c) é simplesmente $(c \bmod sk) \bmod 2$ (Se os textos criptografados da chave pública tiverem baixo ruído, o texto criptografado c vai ter baixo ruído⁴, logo a descriptografia funciona).

Além destas três funções nosso sistema tem uma outra função chamada *Avaluate*. Essa função recebe um circuito⁵ com t entradas e conjunto de textos criptografados $\{c_1, c_2, \dots, c_t\}$ e retorna o resultado do circuito (Operações de soma, subtração e multiplicação). O resultado do circuito descriptografado deve ser igual a saída do circuito com os textos planos como entrada.

Este sistema de criptografia é homomórfico pois podemos somar os textos criptografados como inteiros (Através da função *Avaluate*) e depois descriptografá-los. Isso funciona pois o ruído tem a mesma paridade que o texto original, porém o ruído aumenta a cada operação até que não é retornado o valor certo ao descriptografar.

³A lista tem tamanho polinomial em λ

⁴Ruído é gerado quando um texto é criptografado. Ele se dá por $(c \bmod sk)$

⁵Representado por operações XOR e AND

Para que este sistema seja completamente homomórfico temos que ter uma função que diminua o ruído até que outra operação possa ser executada.

1.4.2 De parcialmente para completamente homomórfico

Antes de continuarmos, vamos definir alguns conceitos sobre nosso sistema de criptografia atual:

- O ruído é inserido durante a criptografia de um bit (Função *Encrypt*);
- A função *Avaluate* pode fazer adições, subtrações e multiplicações, mas o ruído é aumentado respectivamente.
- O sistema consegue descriptografar até uma certa quantidade de ruído, após disso as respostas não são mais confiáveis.
- Inversamente à função *Encrypt*, *Decrypt* retira o ruído.

Para que nosso sistema possa ser completamente homomórfico, a própria função *Decrypt* é usada para diminuir o ruído. Então o sistema deve que ser capaz de computar sua própria função de descriptografar na função *Evaluate*, ou seja, além de somar, subtrair e multiplicar, é necessário suportar a função de descriptografar. A função *Decrypt* removeria o ruído de uma criptografia, mas o texto plano estaria exposto. Logo, temos que descriptografar o texto encriptografado por pk_1 enquanto ele estiver criptografado por pk_2 . Para isso temos a seguinte função:

Recrypt (pk_i , D, sk'_{i-1} , c_{i-1}):

- $c'_{i-1} = \text{Encrypt}(pk_i, c_{i-1,j})$ para $j = 0$ até $j = N$ onde $N = \text{numero de bits de } c_{i-1}$
- Return $c = \text{Evaluate}(pk_i, D, sk'_{i-1}, c'_{i-1})$

Onde: pk_i é uma das chaves públicas, sk'_{i-1} é um vetor em que cada posição é um bit de sk_{i-1} criptografado usando pk_i , D é o circuito que computa a função *Decrypt*, e c_{i-1} é a criptografia de um bit m usando pk_{i-1} .

A função Recrypt primeiramente criptografa cada um dos bits de c_{i-1} , gerando assim um vetor com os bits de c_{i-1} criptografados. Esse vetor, em conjunto com o vetor sk'_{i-1} são usados como entrada para o circuito D , que é executado dentro da função Evaluate. Como a função Decrypt está representado por um circuito binário (D), e como o sistema consegue executar o circuito D sem que o ruído passe do limite, o resultado c de Recrypt é a criptografia de $Decrypt(sk_i - 1, c_{i-1})$ usando pk_i .

Ou seja, o bit m criptografado primeiramente por pk_{i-1} , agora está criptografado por pk_i . Isso é possível pois após Encrypt o texto está duplamente criptografado, e a função Evaluate remove a criptografia mais interna (A por pk_{i-1}). É possível notar que a função Evaluate remove o ruído da criptografia por pk_{i-1} por causa do circuito sendo usado, mas ao mesmo tempo introduz um novo ruído quando avalia a criptografia por pk_i . Desde que o novo ruído inserido seja menor que o ruído removido, podemos continuar aplicando esse processo sem que o ruído passe do limite.

Somente isso não torna o sistema completamente homomórfico, a função Recrypt somente muda da criptografia de uma chave pk_k para pk_{k+1} . Como o objetivo é poder fazer operações nos dados sem que o limite passe do limite, podemos criar um novo circuito que é igual a D , mas com uma operação a mais. Logo, o circuito usado faz a decriptografia e uma operação (Adição ou multiplicação), fazendo com que o sistema seja completamente homomórfico.

A chave pública do sistema consiste de um conjunto de chaves públicas $(pk_1, pk_2, \dots, pk_{n+1})$ e a chave privada consiste de um conjunto de chaves privadas criptografadas $(sk_1, sk_2, \dots, sk_n)$, onde sk_i é criptografada por pk_{i+1} .

1.4.3 Simplificando a decriptografia

Como foi mostrado na seção anterior, se o sistema conseguir executar sua própria função de decriptografar como um circuito binário, então o sistema pode ser transformado em completamente homomórfico. Mas o sistema parcialmente descrito ainda não tem essa característica, então ele foi alterado para um sistema que tenha

a descryptografia simples o suficiente para poder ser executada.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

1.4.4 Como as operações funcionam

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

1.5 Segurança

- probabilidade de 'adivinhar' o plain text e a chave privada - mostrar calculo de probabilidade

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

1.5.1 Ataques conhecidos

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

1.6 Implementação do algoritmo

A implementação usada para testes com criptografia completamente homomórfica foi a biblioteca FHEW⁶ criada por Leo Ducas e Daniele Micciancio baseada no paper Bootstrapping Homomorphic Encryption in less than a second.

1.6.1 O que está implementado

A biblioteca oferece funções para:

- Criar chave secreta e chave pública
- Criptografar bit
- Descriptografar bit crptografado
- Executar um NAND homomórfico em dados criptografados

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

1.6.2 Diferenças entre a implementação e o sistema de Gentry

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

⁶Pode ser encontrada em <https://github.com/lducas/FHEW>

1.7 Testes e Comparações

1.7.1 Arquitetura usada

A arquitetura do computador usada para os testes é a seguinte:

- **Processador:** Intel(R) Core(TM) i5-3337U CPU @ 1.80GHz
- **Memória RAM:** 8,00 GB (7,88 GB utilizáveis)
- **Sistema Operacional:** Debian 7 (64 bits)

1.7.2 Implementação usada para comparação

O algoritmo RSA foi usado como comparação com o sistema completamente homomórfico pois ele é usado em larga escala atualmente, além de ser a origem da CCH. A implementação utilizada foi a *⁷ por ser próxima a um RSA puro (sem otimizações) e por ser na mesma linguagem que a implementação do CCH.

1.7.3 Metodología

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

⁷Pode ser encontrada em *

1.7.4 Resultados

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

1.8 Conclusões

Nunc vitae tincidunt urna. Quisque non rhoncus ligula, eget mattis magna. Proin eget dictum mi. Nulla facilisi. Fusce fermentum tincidunt libero sed aliquam. Fusce in lectus erat. Maecenas blandit, ante ac euismod auctor, turpis purus dictum ligula, vel placerat libero massa ut erat. Donec tristique tincidunt purus vel egestas.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.