XXXIII Congresso de Iniciação Científica da Unicamp

Acelerando criptografia homomórfica baseada em inteiros

Palavras-Chave: Criptografia, Criptografia homomórfica, Fully homomorphic encryption

Autores:

João Pedro Martins Leôncio Eusébio, IC – Unicamp

Prof. Dr. Hilder Vitor Lima Pereira, IC – Unicamp

INTRODUÇÃO:

Contexto e Motivação:

A Criptografia Completamente Homomórfica (CCH) é uma primitiva criptográfica que permite que uma entidade, como um provedor de serviços em nuvem, execute funções computacionais de complexidade arbitrária sobre dados cifrados sem a necessidade de acesso à chave secreta de decifração. O resultado de tal computação permanece cifrado e só pode ser decifrado pelo proprietário dos dados. Esta propriedade única resolve um dos desafios mais persistentes na segurança da informação: proteger os dados em uso. As aplicações potenciais são vastas e impactantes, abrangendo desde a análise segura de dados médicos e financeiros em nuvens públicas até a construção de modelos de aprendizagem de máquina que preservam a privacidade dos dados de treinamento.

A Lacuna de Desempenho e Objetivos do Projeto

Historicamente, os esquemas baseados em LWE receberam maior atenção da comunidade de pesquisa, resultando em avanços significativos em otimização e desempenho. O esquema FHEZ, proposto em (PEREIRA, 2021), representa o estado da arte em CCH sobre inteiros, tendo sido o primeiro a alcançar um tempo de **bootstrapping** inferior a um segundo. No entanto, mesmo com este avanço, o FHEZ permanece ordens de magnitude mais lento do que seus equivalentes baseados em LWE, como o TFHE em (CHILLOTTI et al., 2020).

Este projeto de pesquisa é motivado pela necessidade de diminuir essa lacuna de desempenho. O objetivo geral é aplicar um conjunto de técnicas de otimização para criar uma nova implementação mais eficiente do FHEZ. A linguagem escolhida para criar a base matemática da cifra será Rust, devido à biblioteca **concrete-fft**, capaz de realizar operações de FFT com extrema eficiência. Este relatório

documenta a conclusão da primeira fase deste projeto: a implementação e a verificação de um **backend** aritmético de alto desempenho em Rust que sirva como base para implementação da cifra homomórfica.

REVISÃO TEÓRICA:

A Criptografia Homomórfica sobre os inteiros é fundamentada no problema do Divisor Comum Aproximado (AGCD). O esquema FHEZ, alvo de otimização neste projeto, estende esses conceitos para operar sobre anéis de polinômios com coeficientes inteiros, especificamente em $R = Z[X]/(X^N + 1)$, ou seja, o anel de polinômios em *X* de grau menor que *N*, como descrito em (PEREIRA, 2021).

A representação *double-CRT* aborda o desafio de manipular polinômios com coeficientes extremamente grandes (e.g., >200 bits em FHEZ). A técnica utiliza o Teorema Chinês do Resto para decompor um polinômio com coeficientes em Z_Q em múltiplos polinômios com coeficientes em corpos finitos menores Z_q, que podem ser manipulados por tipos de dados nativos de 64 bits. Cada um desses polinômios é então transformado via FFT. O resultado é que operações complexas se tornam operações ponto a ponto sobre uma matriz de inteiros de 64 bits, eliminando a necessidade de aritmética de precisão arbitrária (GUIMARÃES; PEREIRA; VAN LEEUWEN, 2023).

RESULTADOS E DISCUSSÃO:

A corretude das operações foi verificada através de testes unitários, comparando os resultados das operações em *double-CRT* com uma implementação das mesmas funções, realizada na linguagem Sage. Para validar a eficiência da base aritmética implementada, foram realizados benchmarks preliminares para as operações fundamentais.

Os testes foram executados em um notebook com um processador Intel(R) Core(TM) i5-10210U CPU @ 1.60GHz, utilizando polinômios de grau *N = 32*, coeficientes da ordem de 50 bits e uma base CRT com 10 primos, cada um com um tamanho de 10 bits. Os resultados, que medem o tempo de execução por operação, estão sumarizados na Tabela.

Operação	Tempo Médio	Tempo Mínimo	Tempo Máximo
Polinômio para DCRT	80.828 µs	50.967 µs	179.124 µs
DCRT para Polinômio	289.403 µs	260.047 µs	432.86 µs
Adição em DCRT	1.494 µs	0.939 µs	4.110 µs
Multiplicação em DCRT	1.900 µs	1.065 µs	32.112 µs
Produto Interno	78.101 µs	51.971 µs	176.004 µs
Produto Externo	406.479 µs	348.995 µs	670.339 µs

Tabela 1: Resultados preliminares de benchmark para as operações da base aritmética em DCRT.

CONCLUSÕES:

Este relatório detalhou a conclusão da fase fundamental do projeto que visa acelerar a CCH sobre inteiros. A utilização da representação *double-CRT* em Rust, combinada com uma biblioteca de FFT eficiente, estabelece uma fundação sólida e confiável para as fases subsequentes do projeto. Em última análise, esta pesquisa contribui para o objetivo maior de tornar a CCH sobre inteiros uma alternativa prática e competitiva, fortalecendo o princípio da diversidade de hipóteses no campo da computação segura e com preservação de privacidade.

BIBLIOGRAFIA

PEREIRA, Hilder Vitor Lima. **Bootstrapping fully homomorphic encryption over the integers in less than one second**. In: IACR INTERNATIONAL CONFERENCE ON PUBLIC-KEY CRYPTOGRAPHY, 24., 2021, Edinburgh. Proceedings... Cham: Springer, 2021. p. 331-359.

GUIMARÃES, Antonio; PEREIRA, Hilder V. L.; VAN LEEUWEN, Barry. **Amortized bootstrapping revisited: Simpler, asymptotically-faster, implemented**. In: GUO, Jian; STEINFELD, Ron (Org.). Advances in Cryptology – ASIACRYPT 2023. Singapore: Springer Nature Singapore, 2023. p. 3-35.

CHILLOTTI, Ilaria; GAMA, Nicolas; GEORGIEVA, Mariya; IZABACHÈNE, Malika. **TFHE: Fast Fully Homomorphic Encryption Over the Torus**. Journal of Cryptology, New York, v. 33, p. 34–91, 2020.

BELORGEY, Mariya Georgieva et al. **Revisiting key decomposition techniques for fhe: Simpler, faster and more generic**. Cryptology ePrint Archive, Report 2023/554, 2023. Disponível em: https://eprint.iacr.org/2023/554. Acesso em: 1 ago. 2025.