Universidade de São Paulo
Instituto de Matemática e Estatística
Bachalerado em Ciência da Computação

Gustavo Henrique Muriel Zanon

Criptografia Homomórfica
Parte subjetiva

São Paulo
Novembro de 2016

Apreciação do trabalho

Se eu pudesse resumir o que achei de ter feito esse trabalho em uma palavra, essa palavra seria ”gratificante”.

A teoria do Paillier estava bem descrita tanto no artigo original quanto em artigos que faziam uma análise minuciosa. Sua propriedade homomórfica foi bem explorada tanto na prática quanto na teoria ao longo dos anos, e a implementação foi feita sem maiores problemas com o uso da biblioteca GMP. Ver o funcionamento da implementação e o resultado final do quebra-cabeças de definições, lemas e teoremas necessários para provar os teoremas centrais e a corretude do algoritmo, foi gratificante.

O NTRU por sua vez foi mais desafiador. Os artigos lidos possuiam variantes não somente do algoritmo, mas também da escolha de parâmetros. Dito isso, observou-se uma grande tendência da literatura em adotar o valor de $p = 3$, o que sabemos que limita o número de operações homomórficas. Ao assumirmos na prática que $p > 3$, vimos que falhas ocorriam. Esse problema foi resolvido ao aumentarmos o valor q e a partir disso recorremos à teoria para encontrar um limite superior do quanto q deveria aumentar, o que foi refinado com testes. Por fim, a teoria descrita em ambas as partes de homomorfismo aditivo e multiplicativo foi uma decorrência do entendimento obtido pela teoria básica e observações empíricas. A sensação de ter contribuído na área, mesmo que de forma pequena, foi extremamente gratificante.

Minha maior frustração durante esse trabalho foi não ter produzido uma biblioteca suficientemente eficiente. Eu esperava conseguir otimizar a biblioteca de inteiros de 128 bits com operações de vetorização e trechos em assembly, mas infelizmente não houve tempo hábil, e a alternativa foi usar a biblioteca GMP. Isso resultou em perda de eficiência no NTRU, já que os polinômios passaram a ter coeficientes de tamanho arbitrário.

Disciplinas relevantes

- **MAC0110 - Introdução à Computação:** Importante primeiro contato com algoritmos e linguagem C.

- **MAT0138 - Álgebra I:** Abordou mais profundamente noções simples como mínimo múltiplo comum, máximo divisor comum e números primos. Também, apresentou noções mais complexas (pelo menos na época em que eu estava cursando a disciplina) como função totiente de Euler, pequeno teorema de Fermat, teorema de Carmichael, teorema de Bezóut, teorema Chinês do Resto e algoritmo de Euclides. Esses conceitos permitiram não somente a compreensão do Paillier, mas também de outros criptossistemas que se baseiam na dificuldade do problema da fatoração.

- **MAC0122 - Princípios de Desenvolvimento de Algoritmos:** Introduziu a noção de eficiência de tempo e aprofundou o entendimento de algoritmos e da linguagem C.

- **MAT0139 - Álgebra Linear:** Estabeleceu conceitos de espaços vetoriais, importantes para o entendimento dos reticulados sobre os quais o NTRU é construído.
- **MAC0300 - Métodos Numéricos da Álgebra Linear:** Mostrou os diferentes tipos de normas vetoriais e suas propriedades, utilizadas para compreender parte da teoria que compõe o NTRU.
- **MAT0213 - Álgebra II:** Essencial para o entendimento de grupos sob adição e multiplicação, conceitos utilizados para a definir e classificar os criptossistemas homomórficos. Introduziu também os conceitos de anéis, corpos, ideais, anéis quociente e algoritmo estendido de Euclides, fundamentais para ambos Paillier e NTRU.
- **MAC0338 - Análise de Algoritmos:** Apresentou as classes de complexidade que contém os problemas difíceis nos quais a segurança dos criptossistemas são baseadas, além aprofundar conhecimentos de eficiência de tempo e introduzir eficiência de espaço.
- **MAC0336 - Criptografia e Segurança de Dados:** Fundamentou a teoria da criptografia e apresentou as criptografias de chave pública e assimétrica, bem como seus principais esquemas.

Próximos passos

Desde meu primeiro contato com o Paulo e com a área de criptografia em 2013, tenho em mente seguir na área, com pesquisas e contribuições tanto teóricas quanto de implementação.

Agradecimentos

Aos professores do IME pelo conhecimento passado durante a graduação.

Ao Prof. Dr. Marcos Antonio Simplicio Junior por ter me supervisionado durante este trabalho.

Ao meu cosupervisor/orientador de iniciação científica/*roommate* de conferência/amigo Paulo, que, mesmo a distância, se manteve presente e disposto a me ajudar.

Aos meus pais, Rosângela Cristina Muriel Zanon e Vanderlei da Silva Zanon, pelo sacrifício que fizeram para que eu pudesse entrar em uma faculdade, me formar e ter melhores oportunidades de vida do que eles tiveram.

À minha namorada, família e aos meus amigos por terem aguentado meu estresse, desespero, ansiedade e até auto-piedade durante esses anos. Obrigado por estarem sempre ao meu lado e por terem me ajudado a seguir em frente mesmo quando pensei em desistir.