Abstract

This thesis provides a comprehensive examination of cryptographic key-exchange protocols leveraging algebraic structures for key encoding. The focal point of our investigation is Stickel's protocol. We not only elucidate the protocol but also implement it in Python. Subsequently, we conduct thorough testing and benchmark its execution time, revealing a possible exponential relationship with the input size. This observation aligns with the findings of Myasnikov, Shpilrain, and Ushakov.

The research extends to the exploration of East's work, which offers various presentations of the partition monoid. Furthermore, we delve into specific submonoids, namely $\mathcal{L}_n$, $\mathcal{R}_n$, and the inverse symmetric monoid $\mathcal{I}_n$. For $\mathcal{I}_n$ we conclude that the presentation is not confluent. We ended the study by inferring that the presentation of the partition monoid by East is not complete.

The thesis culminates in the formulation of a complete presentation for the planar rook monoid, a notable submonoid of the partition monoid. This investigation is motivated by the consideration of partition monoid as potential alternative platform for Stickel's protocol. The synthesis of these cryptographic protocols and algebraic structures contributes to a deeper understanding of the interplay between algebraic structures and cryptographic key exchange, paving the way for potential advancements in secure communication protocols.

Keywords: Cryptography, Partition monoid, Planar rook monoid, Rewriting systems, Stickel protocol

Resumo

Esta tese fornece uma análise abrangente de protocolos de troca de chaves criptográficas que utilizam estruturas algébricas para codificação de chaves. O ponto central da nossa investigação é o protocolo de Stickel. Não só elucidamos o protocolo, mas também o implementamos em Python. Posteriormente, realizámos testes abrangentes e avaliámos o tempo de execução, revelando uma possível relação exponencial com o tamanho do input. Esta observação está alinhada com as descobertas de Myasnikov, Shpilrain e Ushakov.

A investigação estende-se à exploração do trabalho de East, que oferece várias apresentações do monoide de partição. Além disso, aprofundámos submonoides específicos, nomeadamente $\mathcal{L}_n$, $\mathcal{R}_n$, e o monoide simétrico inverso $\mathcal{I}_n$. Para $\mathcal{I}_n$, concluímos que a apresentação não é confluente. Terminámos o estudo, inferindo que a apresentação do monoide de partição por East não é completa.

A tese culmina na formulação de uma apresentação completa para o monoide de torre planar, um notável submonoide do monoide de partição. Esta investigação é motivada pela consideração do monoide de partição como potencial plataforma alternativa para o protocolo de Stickel. A síntese desses protocolos criptográficos e estruturas algébricas contribui para uma compreensão mais profunda da interação entre estruturas algébricas e troca de chaves criptográficas, abrindo caminho para possíveis avanços em protocolos de comunicação segura.

Palavras-chave: Criptografia, Monoide de partição, Monoide de torre plana, Protocolo de Stickel, Sistemas de reescrita