Private simultaneous messages based on quadratic residues

Arthur Braga de Campos Tinoco

Arthur Gonçalves de Moraes

Dados

- Autores: Kazumasa Shinagawa, Reo Eriguchi, Shohei Satake, Koji Nuida
- Periódico: Designs, Codes and Cryptography
- Ano de publicação: 2023

Problema abordado no artigo

“Private Simultaneous Messages (PSM)” baseados em resíduos quadráticos (QR-PSM)

Motivação/Objetivo

Desenvolver um protocolo PSM mais eficiente para funções simétricas.

Conclusão

Os autores demonstraram que Ln < P_2^(n - 1) e Ln ≥ 2^((2^n - 2)/n). Foi também demonstrado que $Pn \leq (1 + o(1))n^2 2^{(2n-2)}$, sendo esse o limite superior para os primos de Peralta, através da teoria dos grafos. Como resultado foi obtido o limite inferior para os LQR-PSM primos, sendo também notado que os limites superiores para os primos de Peralta obtidos são estritos que o que foi implicado no resultado do Peralta.