

勉強会形式ゼミ資料②

L. Ducas, L. N. Pulles and M. Stevens Towards a modern
LLL implementation[1]

佐藤 新

July 4, 2025

Seysen 簡約

- $\{b_1, \dots, b_n\}$: 基底
-

参考文献 I

- [1] Léo Ducas, Ludo N. Pulles, and Marc Stevens. Towards a modern LLL implementation. Cryptology ePrint Archive, Paper 2025/774, 2025.