Document title

Author 1

June 27, 2024

1 First section

Definition 1.1 (Lattice)**.** *A lattice is a discrete subgroup of* $\mathbb{R}^n$

Theorem 1.1 (Minkowski's bound)**.** *let* $\mathcal{L}(B)$ *be a full-rank lattice with basis* $B \in \mathbb{R}^{n\times n}$*, and* $B^* = [\mathbf{b}_1^*, \mathbf{b}_2^*, \ldots, \mathbf{b}_n^*]$ *be the Gram-Schmidt orthogonalization of* B*, then*

$$\lambda_1(\mathcal{L}(B)) \geq \min_{1\leq i\leq n} |\mathbf{b}_i^*| \tag{1}$$

Algorithm 1 An algorithm with caption

Require: $n \geq 0$
Ensure: $y = x^n$
  $y \leftarrow 1$
  $X \leftarrow x$
  $N \leftarrow n$
  while $N \neq 0$ **do**
    if N is even **then**
      $X \leftarrow X \times X$
      $N \leftarrow \frac{N}{2}$ ▷ This is a comment
    else if N is odd **then**
      $y \leftarrow y \times X$
      $N \leftarrow N - 1$
    end if
  end while

Here is some citation[FO99]

References

[FO99] Eiichiro Fujisaki and Tatsuaki Okamoto. Secure integration of asymmetric and symmetric encryption schemes. In *Annual international cryptology conference*, pages 537–554. Springer, 1999.