Identity Based Encryption (IBE) from Lattices

Me: Pauline Bert  
Team: EMSEC  
Advisors: Pierre-Alain Fouque and Adeline Roux-Langlois

$Lattice = \text{set of all integer linear combinations of some basis vectors.}$

Given $B = \begin{pmatrix} b_1 \\ b_2 \end{pmatrix}$,

- **Shortest Vector Problem (SVP):**
  find the closest \( \bullet \) from the origin,

- **Closest Vector Problem (CVP):**
  find the closest \( \bullet \) from a targeted \( \bullet \).

\( \rightarrow \) to construct cryptographic primitives (PKE, signature, IBE etc) we need two other problems: the SIS problem, and the LWE problem.

More details on SIS/LWE/IBE in the poster