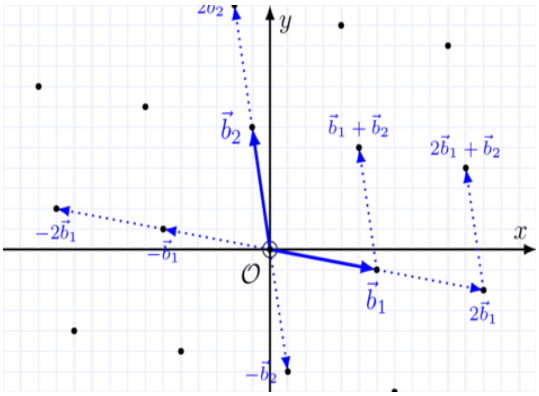
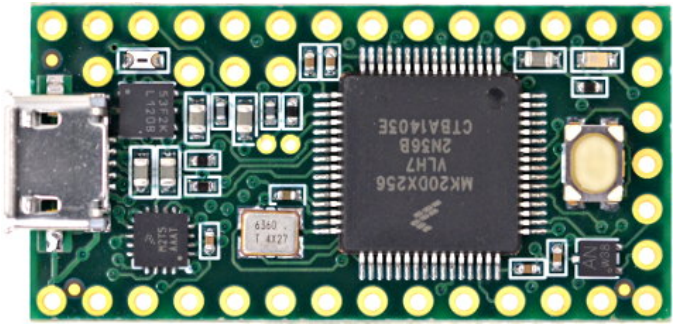
Titre : Euclide Embarqué
Objectif : Implémentation cryptologique sur système embarqué
Encadrant : Guénaël Renault (guenael.renault@gmail.com)

L'objectif de ce projet est l'implémentation d'un échange de clé cryptographique. L'algorithme est basé sur les réseaux euclidiens, objets mathématiques sur lesquels reposent plusieurs systèmes cryptographiques développés récemment (e.g. LWE, NTRU).



Le code sera réalisé en C pour une architecture ARM puisque l'application devra pouvoir tourner sur une Teensy 3.2 (fournies aux étudiants pour la réalisation du projet).



Le cryptosystème à implémenter est NewHope-Simple (https://cryptojedi.org/papers/newhopesimple-20161217.pdf). Il s'agit d'un potentiel candidat pour la compétition permettant de sélectionner de nouveaux cryptosystèmes standardisés par le NIST.