Aspects of code-based cryptography

Mots clés :

- Directeur de thèse : nicolas SENDRIER
- Co-encadrant(s) :
- Unité de recherche : INRIA-Paris
- Ecole doctorale : École Doctorale Informatique, Télécommunications, Électronique de Paris
- Domaine scientifique principal: Divers

Résumé du projet de recherche (Langue 1)
1 Introduction Quantum computers can potentially break most if not all conventional cryptosystems actually deployed in practice, namely, all systems based on the integer factorization problem (like RSA [15]) or the discrete logarithm problem (like traditional or elliptic curve Diffie-Hellman and DSA, and also all of pairing-based cryptography). Certain classical cryptosystems, inspired on computational problems of a nature entirely different from the above and potentially much harder to solve, remain largely unaffected by the threat of quantum computing, and have thus been called quantum-resistant or, more suggestively, ‘post-quantum’ cryptosystems. These include lattice-based cryptosystems and code-based cryptosystems like McEliece [10] and Niederreiter [13].
