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].

Such systems usually have even a speed advantage over conventional schemes; for instance, both McEliece and Niederreiter encryption over a code of length n has time complexity O(n^2), while Diffie-Hellman/DSA and (private exponent) RSA with n-bit keys have time complexity O(n^3), deserving careful attention of the research community. On the other hand, they are plagued by very large keys compared to their conventional counterparts. Many interesting research topics follow from this scenario. 2 Details Some works have been proposed toward the goal of reducing key length of McEliece cryptosystems, like in [12] using low density parity-check codes, in [9] using quasi-cyclic codes, and in [1] using a combination of both. However, these proposals were all shown to contain weaknesses [14]. In those proposals the trapdoor is protected essentially by no other means than a private permutation of the underlying code. The attack strategy consists of obtaining a solvable system of linear equations that the components of the permutation matrix must satisfy, and was successfully mounted due to the very constrained nature of the secret permutation (since it has to preserve the quasi-cyclic structure of the result) and the fact that the secret code is a subcode of a public code. A dedicated fix to the problems in [1] is proposed in [2]. More recently, Berger et al. [4] showed how to circumvent the drawbacks of Gaborit's original soft message attack. I remove the weaknesses pointed out in [14] using this-cyclic codes point out to the impossibility of distinguish punctured codes [16]; 2. Working with subfield subcodes over an intermediate subfield between the base field and the extension field of the original code. These techniques were also applied in [11] using quasi-dyadic codes, representing one of the most prominent results aiming the key length reducing. However, in [6] is presented an attack (reducing the decoding problem to the task of solving multivariate quadratic systems), breaking the parameters proposed over finite fields (but not affecting the binary ones). Several open questions follow from this subject: Which is the exact security properties of quasi-dyadic codes? Is it possible to do the same with different code families as we can do with Goppa ones? Is it possible to further reduce the McEliece key length without sacrificing security? Are there other uses for these codes besides conventional encryption? For digital signature, in [5], Courtois, Finiasz and Sendrier presents one of the most promising schemes known based on the difficulty of decoding linear error-correcting codes. However, it has the drawback that public keys tend to be exceedingly large [8]. Part of its difficulty resides in obtaining codes with high density of decodable syndromes, since the signing mechanism involves sampling random syndromes until a decodable one is found. Essentially the only family of suitable codes for this purpose is that of binary Goppa codes, for which one can correct all t designed errors, leading to a signing complexity of O(t!). The original quasi-dyadic construction only yields codes with a fairly low density of decodable syndromes, comparable to generic alternant codes rather than to other Goppa codes, not fitting for this purpose. In [3] was investigated a variant able to produce codes with a high density of decodable syndromes, relaxing some constraints. This result brings many questions: which is the accurate security of this variant? Is there a way to improve the efficiency of the code generator algorithm? Is it possible to improve the maximum length of the code? Is there an alternative approach to increase the density of structured Goppa codes using codes over a prime characteristic finite field? How can this change affect the proportion of decodable syndromes? Furthermore, an interesting subject comes from the analysis of the attack of Berger et al. [4]. I prove that this attack is infeasible even for very large keys by proving that the secret codes are not distinguishable from random. In particular, this result shows that the McEliece cryptosystem is potentially secure against quantum computers. However, the McEliece cryptosystem is not the only one that is potentially secure against quantum computers; in fact, there are other post-quantum cryptosystems that have similar security properties. These include lattice-based cryptosystems and code-based cryptosystems like McEliece [10] and Niederreiter [13].


Résumé du projet de recherche (Langue 2)