«LA TECHNIQUE DE REPRÉSENTATION - APPLICATION À DES PROBLÈMES DIFFICILES EN CRYPTOGRAPHIE» PAR ANJA BECKER

Présentée par : Anja Becker Discipline : Informatique Laboratoire : PRISM

Résumé :
Cette thèse porte sur les techniques algorithmiques pour résoudre des instances uniformes du problème du sac à dos exact (subset sum) et du décodage à distance d'un code linéaire aléatoire. Le subset sum est une alternative aux problèmes utilisés classiquement en cryptographie (comme le problème de la factorisation et du logarithme discret). Il admet une description simple et ne nécessite de réaliser qu'une somme de nombre entiers. De plus, aucun algorithme quantique polynomial n'est connu pour résoudre ou approcher ce problème. Il est possible de construire des fonctions à sens unique, des générateurs de nombres pseudo aléatoires et des schémas de chiffrement à clé publique dont la sécurité est basée sur la difficulté du problème dans le cas moyen. Les problèmes de décodage peuvent être vus comme une version vectorielle du problème du subset sum. Plus particulièrement le problème du décodage borné dans un code aléatoire, est à la base de plusieurs schémas cryptographiques. Il admet des schémas de chiffrement à clé publique, de signature numérique, d'identification et des

fonctions de hachage. Nous présentons différentes techniques algorithmiques génériques pour résoudre ces problèmes. En utilisant la technique de représentation généralisée, nous obtenons un algorithme pour le problème du subset sum dont la complexité en temps asymptotique est diminuée d'un facteur exponentiel dans le pire des cas. Nous montrons que la même technique s'applique dans le domaine des codes. Ce résultat permet d'améliorer le décodage par ensemble d'information qui résout le problème de décodage dans un code aléatoire. Le nouvel algorithme diminue la complexité en temps asymptotique d'un facteur exponentiel.

Abstract :
The focus of this thesis is an algorithmic technique to solve the random, hard subset-sum problem and the distance-decoding problem in a random linear code. The subset-sum problem provides an alternative to other hard problems used in cryptography (e.g., factoring or the discrete logarithm problem). Its description is simple and the computation of sums of integers is an easy task. Furthermore, no polynomial-time quantum algorithm for solving general knapsacks is known. One can construct one-way functions, pseudo-random generators and private-key encryption schemes from the hardness assumption of the average-case problem. Also some cryptosystems based on lattice problems are provably as secure as the difficulty of the average-case subset-sum problem. Decoding problems can be seen as a vectorial subset-sum problem. Of particular interest is the bounded-distance-decoding problem in a random code. It permits public-key encryption, digital signatures, identification schemes and hash-functions. We present different generic algorithmic tools to solve the above problems. By use of our extended representation technique, we obtain an algorithm of exponentially lower asymptotic running time than previous approaches for the hardest case of a random subset-sum problem. We show that the technique can be applied to the domain of code-based cryptography. This results in improved information-set decoding that solves the distance-decoding problem for random linear codes. The new algorithm is asymptotically faster by an exponential factor.

INFORMATIONS COMPLÉMENTAIRES

Alexander MAY, Professeur des Universités, à l'Université Technique de Darmstadt/Département Informatique - Darmstadt (Allemagne) - Rapporteur
Nicolas SENDRIER, Directeur de Recherche, à l'INRIA - Le Chesnay - Rapporteur
Igor SHPARLINSKI, Professeur des Universités, à l'Université de Macquarie/Département Informatique - Sydney (Australie) - Rapporteur
Antoine JOUX, Professeur Associé, à l'Université de Versailles

Saint-Quentin-en-Yvelines/Laboratoire Parallélisme, Réseaux, Système, Modélisation (PRISM) - Versailles - Directeur de thèse

Daniel AUGOT, Directeur de Recherche, à l'Ecole Polytechnique - Palaiseau - Examinateur

Jean-Sébastien CORON, Maître de Conférences, à l'Université du Luxembourg/Département Informatique - Luxembourg (Grand Duché de Luxembourg) - Examinateur

David NACCACHE, Professeur des Universités, à l'ENS/Département d'Informatique - Paris – Examinateur

Monica NEVINS, Maître de Conférences, à l'Université d'Ottawa/Département de Mathématiques et de Statistique - Ottawa (Canada) - Examinateur

Contact : dredval service FED : theses@uvsq.fr