"ATTAQUES ALGÉBRIQUES DU PROBLÈME DU LOGARITHME DISCRET SUR COURBES ELLIPTIQUES" PAR VANESSA VITSE

Présentée par : Mme Vanessa VITSE Discipline : Informatique Laboratoire : PRiSM

Résumé :
Le sujet principal de cette thèse est le problème du logarithme discret sur courbes elliptiques, d'importance pratique considérable en cryptographie asymétrique. On propose plusieurs nouvelles méthodes pour attaquer ce problème sur des extensions de corps finis. Après une description complète des techniques GHS puis des attaques par décompositions introduites par Gaudry et Diem, on présente des variantes fragilisant le DLP sur courbes elliptiques pour une gamme plus large d'extensions de corps finis. Une nouvelle approche combinant les méthodes de recouvrements et décompositions est aussi proposée : elle permet de résoudre le logarithme discret sur courbes elliptiques pour des extensions sextiques de taille jamais atteinte auparavant. Un ingrédient important est l'utilisation des bases de Gröbner pour la résolution de systèmes polynomiaux ; à cet effet, on introduit un algorithme adapté au contexte de la cryptanalyse algébrique, plus performant dans ce cadre que les algorithmes standards.

Abstract :
The main subject of this Ph.D. thesis is the discrete logarithm problem on elliptic curves, which is of major interest in public-key cryptography. Several new methods for solving this problem over finite field extensions are proposed. After a complete description of the GHS transfer techniques and of the decomposition attacks introduced by Gaudry and Diem, we present variants of these methods, enlarging the range of extension fields over which the elliptic curve DLP is weak. A new approach based on a combination of cover and decomposition methods is also proposed, allowing to compute discrete logarithms on elliptic curves defined over sextic extensions whose sizes had never been reached before. An important ingredient is the use of Gröbner bases for polynomial system solving. We introduce an algorithm optimized for the algebraic cryptanalysis context, that outperforms in this setting standard algorithms.

INFORMATIONS COMPLÉMENTAIRES

Pierrick GAUDRY, Directeur de Recherche, au Laboratoire Lorrain de Recherche en Informatique et ses Applications (LORIA) - UMR 7503 - Vandœuvre-lès-Nancy - Rapporteur
Arjen LENSTRA, Professeur des Universités, à l'Ecole Polytechnique Fédérale de Lausanne/Laboratoire de Cryptologie Algorithmique (LACAL) - Lausanne (Suisse) - Rapporteur
Antoine JOUX, Professeur Associé, à l'Université de Versailles Saint-Quentin-en-Yvelines/Laboratoire Parallélisme, Réseaux, Système, Modélisation (PRiSM) - Versailles - Directeur de thèse
Philippe ELBAZ-VINCENT, Professeur des Universités, à l'Institut Fourier - UMR 5582 - Saint-Martin-d'Hères - Examinateur
Andreas ENGE, Directeur de Recherche, à l'Université de Bordeaux 1/Institut de Mathématiques de Bordeaux - UMR 5251 - Talence - Examinateur
Louis GOUBIN, Professeur des Universités, à l'Université de Versailles Saint-Quentin-en-Yvelines/Laboratoire Parallélisme, Réseaux, Système, Modélisation (PRISM) - Versailles - Examinateur
Grégoire LECERF, Chargé de Recherche CNRS, à l'Ecole Polytechnique/Laboratoire d'Informatique - UMR 7161 CNRS - Palaiseau – Examinateur
Reynald LERCIER, Chercheur, à l'Université de Rennes 1/Institut de Recherche Mathématiques de Rennes (IRMAR) - UMR 6625 CNRS – Rennes - Examinateur

Contact : dredval service FED : theses@uvsq.fr