PRESS RELEASE I PARIS I 09 MAY 2014

New algorithm shakes up cryptography

Researchers at the Laboratoire Lorrain de Recherches en Informatique et ses Applications (CNRS/Université de Lorraine/Inria) and the Laboratoire d'Informatique de Paris 6 (CNRS/UPMC) have solved one aspect of the discrete logarithm problem. This is considered to be one of the 'holy grails' of algorithmic number theory, on which the security of many cryptographic systems used today is based. They have devised a new algorithm (1) that calls into question the security of one variant of this problem, which has been closely studied since 1976. This result, published on the site of the *International Association of Cryptologic Research* and on the HAL open access archive, was presented at the international conference Eurocrypt 2014 held in Copenhagen on 11-15 May 2014 and published in *Advances in cryptology.* It discredits several cryptographic systems that until now were assumed to provide sufficient security safeguards. Although this work is still theoretical, it is likely to have repercussions especially on the cryptographic applications of smart cards, RFID chips (2), etc.

To protect confidentiality of information, cryptography seeks to use mathematical problems that are difficult to solve, even for the most powerful machines and the most sophisticated algorithms.

The security of a variant of the discrete logarithm, reputed to be very complex, has been called into question by four researchers from CNRS and the Laboratoire d'Informatique de Paris 6 (CNRS/UPMC), namely Pierrick Gaudry, Răzvan Bărbulescu, Emmanuel Thomé and Antoine Joux (3). The algorithm they devised stands out from the best algorithms known to date for this problem. Not only is it significantly easier to explain, but its complexity is also considerably improved. This means that it is able to solve increasingly large discrete logarithm problems, while its computing time increases at a far slower rate than with previous algorithms. The computation of discrete logarithms associated with problems that are deliberately made difficult for cryptographic applications is thus made considerably easier.

Since solving this variant of the discrete logarithm is now within the capacity of current computers, relying on its difficulty for cryptographic applications is therefore no longer an option. This work is still at a theoretical stage and the algorithm still needs to be refined before it is possible to provide a practical demonstration of the weakness of this variant of the discrete logarithm. Nonetheless, these results reveal a flaw in cryptographic security and open the way to additional research. For instance, the algorithm could be adapted in order to test the robustness of other cryptographic applications.

(1) A method consisting in a series of instructions that enables a computer to solve a complex problem.

(2) An RFID chip is a computer chip coupled with an antenna that enables it to be activated at a distance by a reader and to communicate with it.

(3) Antoine Joux, who was attached to the Laboratoire Parallélisme, Réseaux, Systèmes, Modélisation (PRISM) (CNRS/UVSQ) at the time of open access publication, is currently a researcher at the Laboratoire d'Informatique de Paris 6 (CNRS/UPMC) and has since obtained the Chair of Cryptology at the Fondation UPMC.

References:

A Heuristic Quasi-Polynomial Algorithm for Discrete Logarithm in Finite Fields of Small Characteristic, Razvan Barbulescu, Pierrick Gaudry, Antoine Joux, Emmanuel Thomé, Advances in Cryptology – EUROCRYPT 2014, Lecture Notes in Computer Science, Volume 8441, 2014, pp 1-16.
dx.doi.org/10.1007/978-3-642-55220-5_1

Contact information

Researchers
Emmanuel Thomé I T +33 (0)3 54 95 86 59 I emmanuel.thome@inria.fr
Pierrick Gaudry I T +33 (0)3 83 59 20 62 I pierrick.gaudry@loria.fr

CNRS Press Office **I** Laetitia Louis **I** T +33 (0)1 44 96 51 37 **I** laetitia.louis@cnrs-dir.fr