A SAT solver is software that checks and ensures the reliability and dependability of computer hardware (processors for example) and software. It can also be used to solve cryptographic problems, such as finding a system’s encryption key. Every year, an international competition is held to compare software of this type, the SAT Race. During the 2009 edition, CryptoMiniSAT obtained the best performances in calculating propositions. It is considerably easier to solve cryptographic problems. And by reasoning at the XDR level, CryptoMiniSAT can outperform other SAT solvers because such problems have a large number of XDR clauses. This is a particularly useful feature when testing installations in operating systems such as Linux. Another strength of the software is algorithms written to force variables to take fixed values, enabling a more accurate approximation of solutions, and a very random search to find solutions more quickly.

CONTACT

Mate Soes, PhD student on the Planète project team, INRIA Grenoble - Rhône Alpes, msoes@lri.fr

CONTACT

Olivier Bernard, Biocore project, INRIA Sophia Antipolis – Méditerranée Tel.: +33 4 93 38 71 85, olivier.bernard@inria.fr