Black-box models of computation in cryptology

Jager, Tibor, author

Abstrak

Generic group algorithms solve computational problems defined over algebraic groups without exploiting properties of a particular representation of group elements. This is modeled by treating the group as a black-box. The fact that a computational problem cannot be solved by a reasonably restricted class of algorithms may be seen as support towards the conjecture that the problem is also hard in the classical Turing machine model. Moreover, a lower complexity bound for certain algorithms is a helpful insight for the search for cryptanalytic algorithms. Tibor Jager addresses several fundamental questions concerning algebraic black-box models of computation : Are the generic group model and its variants a reasonable abstraction? What are the limitations of these models? Can we relax these models to bring them closer to the reality?