Cryptology ePrint Archive: Report 2011/053

Adaptive Pseudo-Free Groups and Applications

Dario Catalano and Dario Fiore and Bogdan Warinschi

Abstract: A computational group is pseudo-free if an adversary cannot find solutions in this group for equations that are not trivially solvable in the free group. This notion was put forth by Rivest as a unifying abstraction of multiple group-related hardness assumptions commonly used in cryptography. Rivest's conjecture that the RSA group is pseudo-free had been settled by Micciancio for the case of RSA moduli that are the product of two safe primes. This result holds for a static setting where the adversary is only given the description of the group (together with a set of randomly chosen generators) and has to come up with the equation and the solution.

In this paper we explore a powerful extension of the notion of pseudo-freeness. We identify, motivate, and study pseudo-freeness in face of adaptive adversaries who may learn solutions to other non-trivial equations before having to solve a new non-trivial equation.

Our first contribution is a carefully crafted definition of adaptive pseudo-freeness that walks a fine line between being too weak and being unsatisfiable. We give generic constructions that show how any group that satisfies our definition can be used to construct digital signatures and network signature schemes.

Next, we prove that the RSA group meets our more stringent notion of pseudo-freeness and as a consequence we obtain different results. First, we obtain a new network (homomorphic) signature scheme in the standard model. Secondly, we demonstrate the generality of our framework for signatures by showing that all existing strong RSA-based signature schemes are instantiations of our generic construction in the RSA group.

Category / Keywords: public-key cryptography / pseudo-free groups, RSA, digital signatures

Publication Info: This is the full version of the paper that will appear at Eurocrypt 2011

Date: received 27 Jan 2011

Contact author: dario fiore at ens fr

Available formats: PDF | BibTeX Citation

Version: 20110128:025731 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]