Cryptology ePrint Archive: Report 2011/009

Progression-Free Sets and Sublinear Pairing-Based Non-Interactive Zero-Knowledge Arguments

Helger Lipmaa

Abstract: In 2010, Groth constructed the only previously known sublinear-communication NIZK circuit satisfiability argument in the common reference string model. We optimize Groth's argument by, in particular, reducing both the CRS length and the prover's computational complexity from quadratic to quasilinear in the circuit size. We also use a (presumably) weaker security assumption, and have tighter security reductions. Our main contribution is to show that the complexity of Groth's basic arguments is dominated by the quadratic number of monomials in certain polynomials. We collapse the number of monomials to quasilinear by using a recent construction of progression-free sets.

Category / Keywords: Additive combinatorics, bilinear pairings, circuit satisfiability, non-interactive zero-knowledge, progression-free sets

Publication Info: TCC 2012. This is the corresponding full version.

Date: received 5 Jan 2011, last revised 5 Jan 2012

Contact author: helger lipmaa at gmail com

Available formats: PDF | BibTeX Citation

Note: 19.06.2011 update: Includes many readability updates. The most noteworthy new result: the prover's computational complexity in the new SAT argument is $\Theta (n^2)$ additions (not $\Theta (n^2)$ multiplications, as claimed before).

Version: 20120105:184647 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]