Cryptology ePrint Archive: Report 2013/121

Succinct Non-Interactive Zero Knowledge Arguments from Span Programs and Linear Error-Correcting Codes

Helger Lipmaa

Abstract: Recently, Gennaro, Gentry, Parno and Raykova~\cite{eprint2012:GennaroGPR} proposed an efficient non-interactive zero knowledge argument for Circuit-SAT, based on non-standard notions like conscientious and quadratic span programs. We propose a new non-interactive zero knowledge argument, based on a simple combination of \emph{standard} span programs (that verify the correctness of every individual gate) and high-distance linear error-correcting codes (that check the consistency of wire assignments). We simplify all steps of the argument. As one of the corollaries, we design an (optimal) wire checker, based on systematic Reed-Solomon codes, of size $8 n$ and degree $4 n$, while the wire checker from~\cite{eprint2012:GennaroGPR} has size $24 n$ and degree $76 n$, where n is the circuit size. Importantly, the new argument has constant verifier's computation.

Category / Keywords: cryptographic protocols / Circuit-SAT, linear error-correcting codes,non-interactive zero knowledge, polynomial algebra, span program, verifiable computation

Date: received 28 Feb 2013

Contact author: helger lipmaa at gmail com