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

Helger Lipmaa
University of Tartu
Tartu, Estonia

Recently, Gennaro, Gentry, Parno and Raykova [1] 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 *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 $8n$ and degree $4n$, while the wire checker from [1] has size $24n$ and degree $76n$, where n is the circuit size. Importantly, the new argument has constant verifier's computation.

References

[1] R. Gennaro, C. Gentry, B. Parno, and M. Raykova, Quadratic Span Programs and Succinct NIZKs without PCPs. Technical Report 2012/215, International Association for Cryptologic Research, April 19, 2012. Available at http://eprint.iacr.org/2012/215 .