Diplomarbeit – Roadmap

June 15, 2012

This writing describes the process of securely evaluating arithmetic circuits such as $f(x, y) = ...$ over fields.

1 From Arithmetic Circuits To Matrices

This section will describe how to describe the evaluation of an arithmetic circuit using matrix multiplication [1].

2 Grouping the Matrices

This section will describe how to build groups of matrices which could be evaluated directly using one OAFE application.

3 Garbling the Matrices

This section will describe the process of garbling the matrices.

4 Evaluating them using OAFEs (David & Goliath)

This section will describe how we put everything together.

References

[1] R. Cleve. Towards optimal simulations of formulas by bounded-width programs. *Computational Complexity*, 1(1):91–105, 1991.