Optimal Structure-Preserving Signatures

Jens Groth

University College London, UK
j.groth@ucl.ac.uk

Abstract. Structure preservation captures the notion of pairing-based schemes that rely on generic group operations and where the components are group elements. Their structural properties make it easy to compose them with other pairing-based schemes.

In this talk, we will take a closer look at structure-preserving signatures. The structure preserving property allows us to analyze the efficiency of signature schemes in the generic group model. Using the generic group model to analyze the efficiency of a cryptographic scheme stands in contrast to the more common usage of the generic group model to rule out certain types of attack. We will show that structure-preserving signatures need to consist of at least 3 group elements.

We also discuss recent constructions of structure-preserving signatures that consist of 3 group elements. These constructions match our lower bounds, thus giving us provably optimal structure-preserving signatures.

Keywords: Structure-preserving pairing-based cryptography, digital signatures, generic group model, lower bounds.

X. Boyen and X. Chen (Eds.): ProvSec 2011, LNCS 6980, p. 1, 2011.