Cryptology ePrint Archive: Report 2013/186

On the (Im)possibility of Projecting Property in Prime-Order Setting

Jae Hong Seo

Abstract: Projecting bilinear pairings have frequently been used for designing cryptosystems since they were first derived from composite order bilinear groups. There have been only a few studies on the (im)possibility of projecting bilinear pairings. Groth and Sahai (EUROCRYPT 2008) showed that projecting bilinear pairings can be achieved in a prime-order group setting. They constructed both projecting asymmetric bilinear pairings and projecting symmetric bilinear pairings, where a bilinear pairing e is symmetric if it satisfies $e(g,h)=e(h,g)$ for any group elements g and h; otherwise, it is asymmetric. Subsequently, Freeman (EUROCRYPT 2010) generalized Groth-Sahai's projecting asymmetric bilinear pairings.

In this paper, we provide impossibility results on projecting bilinear pairings in a prime-order group setting. More precisely, we specify the lower bounds of

1. the image size of a projecting asymmetric bilinear pairing

2. the image size of a projecting symmetric bilinear pairing

3. the computational cost for a projecting asymmetric bilinear pairing

4. the computational cost for a projecting symmetric bilinear pairing

in a prime-order group setting naturally induced from the k-linear assumption, where the computational cost means the number of generic operations.

Our lower bounds regarding a projecting asymmetric bilinear pairing are tight, i.e., it is impossible to construct a more efficient projecting asymmetric bilinear pairing than the constructions of Groth-Sahai and Freeman. However, our lower bounds regarding a projecting symmetric bilinear pairing differ from Groth and Sahai's results regarding a symmetric bilinear pairing; We fill these gaps by constructing projecting symmetric bilinear pairings.

In addition, on the basis of the proposed symmetric bilinear pairings, we construct more efficient instantiations of cryptosystems that essentially use the projecting symmetric bilinear pairings in a modular fashion. Example applications include new instantiations of the Boneh-Goh-Nissim cryptosystem, the Groth-Sahai non-interactive proof system, and Seo-Cheon round optimal blind signatures proven secure under the DLIN assumption. These new instantiations are more efficient than the previous ones, which are also provably secure under the DLIN assumption. These applications are of independent interest.

Category / Keywords: Bilinear Groups, Projecting, (im)possibility, Zero-Knowledge Proofs

Publication Info: This is a full version of the extended abstract published in the proceeding of ASIACRYPT 2012

Date: received 1 Apr 2013, last revised 2 Apr 2013

Contact author: jhsbhs at gmail com

Available formats: PDF | BibTeX Citation

Version: 20130403:022816 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]