Resume for Johan Wallen's survey of short signatures from bilinear pairings.

Tatiana Issaeva,

February 1, 2003

1 Content overview

The survey under review concentrates on the results obtained in the article [1]. The article [1] introduces a new signature scheme, which is based on assumption that Computational Diffie-Hellman (CDH) problem is hard for bilinear pairings.

In the introduction part of survey Johan gives a good overview of the problem and also gives all the basic definitions, which are needed for a better understanding of the problem domain for the reader. Johan also provides the references to the other cryptographic problems, which are used to obtains the security proof of presented signature scheme. Also in his introducton to the survey Johan makes a very good remark that results from [1] are one of the first constructive applications of biliners pairings in cryptography.

In the survey introduction Johan names the possible practical applications for the presented signature scheme, as well as provides the pointers for the existing signature schemes and very briefly compares them. One of points which would be good to add to the survey is to extend this comparison with some conctere numbers. It will give a better idea to the reader if survey provides some concrete numbers about the actual size of short signatures, which can be received from the scheme proposed in [1], as compared to the other well known signature schemes. For example a short table as the one shown below would help the reader to see what are the benefits of the signature scheme under consideration in terms signature size.

Scheme	Signature size
RSA	1024
DSA	320
Short Signature from Pairings	160

For other table's example see [2].

To explain the main mathematical results from [1] the survey splits the problem presentation into very good structure and devotes a separate section for every step of the problem domain. The definition of the gap Diffies-Hellman (GDH) groups, the gap signarute scheme definition, its securiry definition and secutiry proof are all presented into separate sections. The survey gives only general definitions of the signature scheme and leaves out the conctere examples of constructing GDH groups from elliptic curves as presented in [1]. Nevertheless, the reader is informed about the latter and given the reference to follow.

The definition of GDH group in [1] is given for the case of two cyclic multiplicate groups G_1 and G_2 and their bilinear pairing $e : G_1 \times G_2 \to G_T$. Johan reduces the general definition given in [1] to the case, when $G_1 = G_2$. To my opinion such simplification is right decision since the general case is only needed when demonstrating the results for certain families of elliptic curves. Since those are left out of the survey, the case of $G_1 = G_2$ will only benefit the reader and ease the understanding of the main results. All the subsequent definitions and proofs are also reduced to the case of $G_1 = G_2$. The security proof of short signature scheme presented in survey by Johan (proof of theorem 7) is significatly extended variant of proof given in [1]. While proof in [1] is more formal, in his survey Johan tries to abstract from the formal notation and give the reader also some intuitive understanding of the proof. I think that he suceeds in this very well.

Overall the survey presents results from [1] very clearly. The only missing thing, which would be good to add to the end survey is one more section that will provide some conclusion to the presented results. Or maybe also name some further extensions, which are followed from results presented in [1], like blind signatures or threshold signatues.

I think it is also worth mentioning the implementaions results. Reference [2] provides some information on it as well as [1].

2 Editorial remarks

This section presents some editorial remarks to the Johan's survey.

After definition 1 there are some notation given to denote that x is choosen from A. Would it be good to use some other letter then A, since imidiately after definition 1 A is used to denote algorithm in definition 2 and this makes a bit confusing notation.

Definition 2, page 2: choice of (a, b) is uniform. This is missing from the definition.

Section 5. Security proof. Should the theorems have their own separate numbering? In this case Theorem 7 should be Theorem 1.

Section 5.1. Second sentence has reference to the theorem, but not its number.

References

[1] B.Bohen, B.Lynn, H.Shacham. “Short signatures from the Weil Pairings”

[2] http://rooster.standford.edu/~ben/crypto/ac01talk/index.html