T-79.512 Cryptology: Special Topics / Pairing-based Cryptography:
Comments on "Bilinear Pairings"

Johan Wallén

January 27, 2003

1 Introduction

In this note, we give some comments on Sven Laur's survey *Bilinear Pairings*. The comments refer to a draft of the survey dated 22.1.2003. The survey presents a brief introduction to bilinear pairings as defined in pairing-based cryptography.

The survey starts with the definition and immediate properties of pairings, and points out their connection with scalar products and discrete logarithms. After that, the survey takes a closer look on various reduction between the discrete logarithm and decisional Diffie-Hellman (DDH) problems in G_1 and G_2 given a pairing $\hat{e}\colon G_1^2 \to G_2$. Since the existence of $\hat{e}$ implies that the DDH is easy in G_1, the survey continues with a discussion of the difficulty of the computational Diffie-Hellman (CDH) problem in G_1. The survey closes with the bilinear Diffie-Hellman (BDH) problem and how it can be used to construct a static 3-party key exchange protocol.

2 General comments

In general, the selection of topics in the survey is good and the level of detail is suitable considering the page limitations. The discussion of the Diffie-Hellman problem in Section 4 would need more details, since this is by far the most complicated part of the survey. A short explanation of the intuition behind the α-efficient parametric embeddings and (m, α)-algebraically defined groups would improve the readability considerably and would make Theorem 2 easier to understand. It would be nice to have a more detailed proof sketch of Theorem 2. What is the input and output of the algorithm? What does steps 2 and 3 of the algorithm really do? The explanation after the algorithm should be more detailed. What is the intuition behind Theorem 2? Some examples would make Section 4 easier to understand.

Section 5 lists several applications of the BDH assumption. It would be nice with references for these applications, although it is not strictly necessary, since they will be covered in later surveys. A textual description of the key exchange protocols in Section 6 would be nice. The figures are enough for readers already familiar with standard 3-party Diffie-Hellman key exchange, but it might be difficult to understand what is going on based only on the figures. It should at least be mentioned what the agreed key is.

It might be good to define the term *gap Diffie-Hellman group*, i.e. a group where DDH is easy but CDH is hard, since the terminology will probably be used a lot in upcoming seminars. Some examples of conjectured gap groups like certain supersingular elliptic curves could also be listed.

3 Specific comments

In this section, we give more detailed comments on the survey, list some (but not all) typos, and suggest some minor additions.

Language Pay attention to the use of articles (the, a, an) and the use of plural forms. For example, in the first sentence one should have 'since the early days' and 'the intractability of the discrete logarithm problem' (or 'the intractability of computing discrete logarithms'). As a quick and dirty rule, articles are used before countable nouns (countable as opposed to substances like water that cannot be counted) in singular form and when referring to a specific object or an object as a representative for a class. A thorough source on this and related topics is [2].

Section 1 (Introduction) *First sentence:* The word 'key' is missing from 'public key cryptography'. *Row 8:* Weil pairing. Some general references on Weil and Tait pairings like [1] would be nice, since they are mentioned but not explained at all.

Section 2 (Definitions and implications) It is mentioned that the definition of bilinear pairings is quite strange (or rather restrictive) from an algebraic point of view (especially the restrictions on the group orders). This could be elaborated slightly. One could perhaps give some interesting examples of (more general) bilinear pairings from some branch of algebra. The first example that comes to mind is the tensor product of vector spaces, but it is probably not that interesting in this context. A trivial example is of course $(x, y) \mapsto xy$ in a ring. In the connection to scalar products, the triviality of the connection could be stressed to improve readability.

The non-degeneracy bullet: Without parenthesis, the property could be interpreted as $\forall T \in G_1 : (\hat{e}(S,T) = 1 \Rightarrow S = 0)$ instead of the intended $(\forall T \in G_1 : \hat{e}(S,T) = 1) \Rightarrow S = 0$. *Row 4 after the non-degeneracy bullet:* Two subgroups. *Page 2, row 8:* 'See' or 'interpret' instead of 'watch'.

Section 3 (Various reductions) The notation G^* for arbitrary groups should probably be defined. *The proof of Proposition 1, last sentence:* It would be clearer to explicitly write f_0 for the zero homomorphism or call it the one homomorphism instead (since it maps everything to 1). An alternative and general name would be the trivial homomorphism.

Section 4 (Diffie-Hellman problem) Define the notation $\mathbb{P}$. Since the implicit representation $y \rightsquigarrow a$ is not widely known and can be a bit confusing when first encountered, some examples would be nice. It would also be nice to elaborate on the implicit representation of arithmetic operations (this could also serve as examples). The notation $DH(a, b)$ is quite obvious, but should still be explained.

Some examples of probabilistically α-efficient parametric embeddings and strongly (m, α)-algebraically defined groups would make the construction much easier to understand and give some intuition for the reduction. This would also give a (perhaps trivial) example of a group where the CDH problem is equivalent to the discrete logarithm problem.

The embedding: A `\mathbb` is missing from $\mathcal{E}mb\colon \mathbb{F}_p \times \mathbb{F}_p \to H$ (two occurrences). *Theorem 2:* B smooth should probably be defined. How are P and g related? Incremental revealing should probably be explained briefly (or not mentioned at all).

Section 5 (Bilinear Diffie-Hellman problem) The definition of the BDH problem is given in more detail, including the advantage (i.e. success probability), than the previous problems like CDH. For consistency, it would be nice to give all the definitions in the same level of detail (and using similar formulations).

Strictly speaking, Corollary 6 only show that BDH *might* be harder that CDH.

Section 6 (Three-party key agreements) The figures describing the protocols are very clear. *Row 2:* Two rounds.

References The author of [M02] is of course Menezes.

4 Minor details

There are some minor inconsistencies in the citation labels (for example, the missing year in [MOV] and the conflicting years in [MW98]). These and similar annoyances are easy to avoid by managing citations using BibTeX.

References

[1] J.H. Silverman. *The Arithmetic of Elliptic Curves.* Springer, 1986.

[2] *The Chicago Manual of Style*. The University of Chicago Press, 14th edition, 1993. See also `http://www.press.uchicago.edu/Misc/Chicago/cmosfaq/cmosfaq.html`.