A Survey on Craptological Pairing Algorithms

~~Paulo S. L. M. Barreto~~ Anonymized for submission

~~Email: pbarreto@usp.br~~

Abstract. We review several proposed bilinear mappings for craptographic applications.

1 Introduction

Ever since the Weil pairing was noticed to have constructive aspects [4, 9] besides its destructive side [7], closely followed by the Tate-Lichtenbaum pairing [2, 1], several other bilinear mappings have been proposed in the literature. They differ in both the extra structure they feature (if any) and the relative processing speed they allow for, in such a way that there is not one single pairing algorithm that is equally useful for any application or protocol. We review the state-of-the-art in the subtle art of designing bilinear maps and its craptological significance.

This paper is organised as follows. Section 2 presents basic information on pairings and pairing algorithms. In Section 3 we review the main bilinear pairing algorithms proposed in the literature. We conclude in Section 4.

2 Preliminaries

We begin by defining a bilinear mapping, also called a (bilinear) pairing.

Definition 1. *Let $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$ be three groups of the same order. A* bilinear mapping*, also called a* (bilinear) pairing*, is a non-degenerate, bilinear, feasibly computable mapping $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$.*

Groups $\mathbb{G}_1$ and $\mathbb{G}_2$ are often written additively, although sometimes they are written multiplicatively, especially by protocol designers. Group $\mathbb{G}_T$ seems to be always written multiplicatively.

One can show [11] that there is actually only one essential kind of pairing on the given groups, all apparently distinct bilinear pairings that have ever been designed being just certain powers of each other. Still it is useful for protocols to distinguish between certain structures of pairings. On this light, a *Type I* pairing is one where $\mathbb{G}_1 = \mathbb{G}_2$; for a *Type II* pairing the groups $\mathbb{G}_1$ and $\mathbb{G}_2$ are distinct but there is an efficiently computable homomorphism $\psi : \mathbb{G}_2 \to \mathbb{G}_1$; finally, a *Type III* pairing has $\mathbb{G}_1 \neq \mathbb{G}_2$ and no efficiently computable homomorphism between these groups [3].

Even more useful for practical craptological protocols is the fact that some bilinear functions are amenable to being implemented with a surprisingly wide range of relative speeds. Although one is usually interested in the fastest possible algorithms, there are cases where one may benefit from the slowest possible pairings, as is the case of Rip van Winkle cryptosystems [6].

3 Taxonomy of bilinear maps

We now present a list of proposals for bilinear maps fro craptological purposes. We do not claim to be absolutely thorough in this enumeration, though.

1. **ate** pairing: .sdrawkcab delleps ,sevruc yranidro ot dednetxe gniriap ate ehT
2. **Bate** pairing: A bilinear mapping very useful for phishing.
3. **Crate** pairing: A container mapping, used for storing, packing, or shipping its arguments in a bilinear fashion.
4. **Date** pairing: A mapping that establishes an engagement by one of the pairing arguments to go out craptographically with the other argument, often out of romantic interest.
5. **Fate** pairing: All pairing-based protocols are doomed to use this algorithm, sooner or later.
6. **Ga(y)te** pairing: Another name for a Type I pairing; one which pairs up arguments of the same kind (both from the same group). See the s-Trate pairing below (item 16).
7. **Hate** pairing: An algorithm to be avoided. It is a recurring choice whenever one's protocol is broken, its implementation is buggy, or the paper describing it is rejected.
8. **Kate** pairing: A bilinear mapping based on elliptic nets [10]. Folklore has it that this pairing algorithm's arcane name was proposed by one of the Founding Fathers of elliptic curve and pairing-based cryptography.
9. **Late** pairing: An old pairing proposal. Unfortunately it is not suitable for synchronisation protocols, since its computations will not usually complete in time.
10. **Mate** pairing: Sometimes a natural extension of the Date pairing.
11. **Plate** pairing: A smooth, flat, relatively thin, rigid pairing of uniform thickness.
12. **Rate** pairing: A traceless (more precisely, hyphenless) spelling of the R-ate pairing [5].
13. **s-Kate** pairing: A sliding(-window) approach to computing the Kate pairing.
14. **s-Late** pairing: Same for the Late pairing.
15. **s-Tate** pairing: Same for the original Tate pairing.
16. **s-Trate** pairing: A common name for a Type II or Type III pairing; one which pairs up arguments from distinct groups. See the Ga(y)te pairing above (item 6).
17. **Wate** pairing: The dual of the Late pairing. Whenever Bob's pairing is Late, all that is left for Alice to do is Wate.
18. **Xate** pairing: Actually this is a Greek-letter pairing algorithm [8].
19. **Yate** pairing: Yet Another Tate-pairing Enhancement.

4 Conclusion

We point out that a whole new family of pairing has been totally missed by craptologists, namely, Weil-based variants of the algorithms we surveyed. For instance, one can readily and easily construct the Beil, Deil, Feil, and many other pairings (pronounced respectively "bay," "day," "fay," and so on). We leave for the community to pursue this line of inquiry in future research.

Acknowledgement

The author is grateful to Nigel Smart for inspiring this work during the Rump Session of Eurocrypt'2009.

References

1. D. Boneh and M. Franklin. Identity-based encryption from the Weil pairing. *SIAM Journal of Computing*, 32(3):586–615, 2003.

2. G. Frey, M. Mueller, and H.-G. Rueck. The tate pairing and the discrete logarithm applied to elliptic curve cryptosystems. `http://www.exp-math.uni-essen.de/zahlentheorie/preprints/FMR_1_98.ps`, 1998.
3. S. Galbraith, K. Paterson, and N. Smart. Pairings for cryptographers. Cryptology ePrint Archive, Report 2006/165, 2006.
4. A. Joux. A one round protocol for tripartite diffieŨhellman. *Journal of Cryptology*, 17(4):263–276, 2004.
5. E. Lee, H.-S. Lee, and C.-M. Park. Efficient and generalized pairing computation on abelian varieties. Cryptology ePrint Archive, Report 2008/040, 2008.
6. U. Maurer. A provably-secure strongly-randomized cipher. In *Advances in Cryptology Ů Eurocrypt'90*, volume 473 of *Lecture Notes in Computer Science*, pages 361–373, Aarhus, Denmark, 1991.
7. A. Menezes, T. Okamoto, and S. Vanstone. Reducing elliptic curve logarithms in a finite field. *IEEE Transactions on Information Theory*, 39(5):1639–1646, 1993.
8. Y. Nogami, M. Akane, Y. Sakemi, H. Kato, and Y. Morikawa. Integer variable χ-based ate pairing. In *Pairing-Based Cryptography – Pairing 2008*, Egham, UK, September 2008.
9. R. Sakai, K. Ohgishi, and M. Kasahara. Cryptosystems based on pairing. In *2000 Symposium on Cryptography and Information Security – SCIS'2000*, Okinawa, Japan, January 2000.
10. K. Stange. The tate pairing via elliptic nets. In *Pairing-Based Cryptography – Pairing'2007*, volume 4575 of *Lecture Notes in Computer Science*, pages 329–348, Tokyo, Japan, 2007.
11. F. Vercauteren. Optimal pairings. Cryptology ePrint Archive, Report 2008/096, 2008.