CO789 Project Descriptions

Student evaluations in CO789 will be based on a final project. The project involves a one hour presentation, to be given in class during the last three weeks of classes, plus a written report on your presentation. Generally the project should be on a topic that goes beyond the scope of the core material presented in the class. Included in this document are some possible ideas for final projects, along with a few references to get you started. If you wish to present some other topic which is not listed here, you are actively encouraged to do so, but please discuss the topic with me in my office beforehand.

Pairing friendly curves: The last couple of years have seen dramatic progress in the construction of efficient pairing friendly curves. Articles include the groundbreaking work of Barreto and Naehrig [2], as well as the comprehensive classification of Freeman, Scott, and Teske [8].

Optimized Tate pairing implementations: A number of enhancements have been discovered to speed up Miller's algorithm for evaluating Weil and Tate pairings and allow for faster performance. Starting points for this topic include [6], [7], and [9].

Eta and ate pairings: The eta [1] and ate [11] pairings are two new cryptographic pairings based upon the Tate pairing (hence the similarity in names). In many cases these pairings offer dramatic performance improvements over the classical Tate pairing.

Generalizations to hyperelliptic curves: It is a relatively new result that cryptography on the Jacobian of a genus 2 or 3 hyperelliptic curve can in many cases outperform elliptic curve cryptography at the same level of security. Papers such as [10] and [14] are representative of recent advances in this area.

Improvements in curve generation: In generating elliptic curves via the CM method, it is possible to save a constant but significant factor in the running time by using other modular class polynomials in place of the traditional Hilbert class polynomial. The IEEE P1363 standard [12] describes one such algorithm based on Weber functions, and [13] provides a good overview of this family of techniques.

Pairing based protocols: A tremendous amount of research is devoted to constructing new protocols and cryptographic primitives using pairings as a building block. Examples of such protocols include blind signatures [15, 16], group signatures [4], threshold signatures [3], and broadcast encryption [5].

References

[1] Paulo S. L. M. Barreto, Steven Galbraith, Colm Ó hÉigeartaigh, and Michael Scott, *Efficient pairing computation on supersingular abelian varieties* (2004). `http://eprint.iacr.org/2004/375/`.

[2] Paulo S. L. M. Barreto and Michael Naehrig, *Pairing-friendly elliptic curves of prime order*, Selected areas in cryptography, Lecture Notes in Comput. Sci., vol. 3897, Springer, Berlin, 2006, pp. 319–331.

[3] Alexandra Boldyreva, *Threshold signatures, multisignatures and blind signatures based on the gap-Diffie-Hellman-group signature scheme*, Public key cryptography—PKC 2003, Lecture Notes in Comput. Sci., vol. 2567, Springer, Berlin, 2002, pp. 31–46.

[4] Dan Boneh, Xavier Boyen, and Hovav Shacham, *Short group signatures*, Advances in cryptology—CRYPTO 2004, Lecture Notes in Comput. Sci., vol. 3152, Springer, Berlin, 2004, pp. 41–55.

[5] Dan Boneh, Craig Gentry, and Brent Waters, *Collusion resistant broadcast encryption with short ciphertexts and private keys*, Advances in cryptology—CRYPTO 2005, Lecture Notes in Comput. Sci., vol. 3621, Springer, Berlin, 2005, pp. 258–275.

[6] Iwan Duursma and Hyang-Sook Lee, *Tate pairing implementation for hyperelliptic curves* $y^2 = x^p - x + d$, Advances in cryptology—ASIACRYPT 2003, Lecture Notes in Comput. Sci., vol. 2894, Springer, Berlin, 2003, pp. 111–123.

[7] Kirsten Eisenträger, Kristin Lauter, and Peter L. Montgomery, *Fast elliptic curve arithmetic and improved Weil pairing evaluation*, Topics in cryptology—CT-RSA 2003, Lecture Notes in Comput. Sci., vol. 2612, Springer, Berlin, 2003, pp. 343–354.

[8] David Freeman, Michael Scott, and Edlyn Teske, *A taxonomy of pairing-friendly elliptic curves* (2006). `http://eprint.iacr.org/2006/372/`.

[9] Steven D. Galbraith, Keith Harrison, and David Soldera, *Implementing the Tate pairing*, Algorithmic number theory (Sydney, 2002), Lecture Notes in Comput. Sci., vol. 2369, Springer, Berlin, 2002, pp. 324–337.

[10] Cyril Guyot, Kiumars Kaveh, and Vijay M. Patankar, *Explicit algorithm for the arithmetic on the hyperelliptic Jacobians of genus 3*, J. Ramanujan Math. Soc. **19** (2004), no. 2, 75–115.

[11] Florian Hess, Nigel Smart, and Frederik Vercauteren, *The eta pairing revisited* (2006). `http://eprint.iacr.org/2006/110/`.

[12] IEEE P1363, *Standard Specifications for Public Key Cryptography*. `http://grouper.ieee.org/groups/1363/P1363/draft.html`.

[13] Elisavet Konstantinou, Aristides Kontogeorgis, Yannis C. Stamatiou, and Christos Zaroliagis, *Generating prime order elliptic curves: difficulties and efficiency considerations*, Information security and cryptology—ICISC 2004, Lecture Notes in Comput. Sci., vol. 3506, Springer, Berlin, 2005, pp. 261–278.

[14] Tanja Lange, *Formulae for arithmetic on genus 2 hyperelliptic curves*, Appl. Algebra Engrg. Comm. Comput. **15** (2005), no. 5, 295–328.

[15] Tatsuaki Okamoto, *Efficient blind and partially blind signatures without random oracles*, Theory of cryptography, Lecture Notes in Comput. Sci., vol. 3876, Springer, Berlin, 2006, pp. 80–99.

[16] Fangguo Zhang and Kwangjo Kim, *Efficient ID-based blind signature and proxy signature from bilinear pairings*, Information security and privacy—ACISP 2003, Lecture Notes in Comput. Sci., vol. 2727, Springer, Berlin, 2003, pp. 312–323.