More constructing pairing-friendly elliptic curves for cryptography

Tanaka Satoru and Nakamula Ken

Department of Mathematics and Information Sciences, Tokyo Metropolitan University,
1-1 Minami Osawa, Hachioji-shi, Tokyo, 192-0397 Japan
satoru@tnt.math.metro-u.ac.jp, nakamula@tnt.math.metro-u.ac.jp

To construct elliptic curves suitable for pairing applications, we propose a variant algorithm of a known method by Brezing and Weng. We produce new families of parameters using our algorithm for pairing-friendly elliptic curves of embedding degree 8, and we actually compute some explicit curves as numerical examples published in [4, 3].

Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$, and r be the largest prime dividing $\#E(\mathbb{F}_q) = q + 1 - t$, the order of the group of $\mathbb{F}_q$-rational points of E with the Frobenius trace t. We define the *embedding degree* by the smallest positive integer k such that r divides $q^k - 1$. The parameters required to determine pairing-friendly elliptic curves are t, r, q, k and the CM discriminant D for the CM method to construct elliptic curves.

We study the problem of computing suitable parameters t, r, q from given parameters k, D. We employ the method proposed in [2, 1] which generates a family of pairing-friendly curves by considering t, r, q as polynomial $t(x), r(x), q(x)$ of a new parameter x. We restrict the embedding degree to $k = 8$ and the CM discriminant to $D = 1$. The key point is how to choose a good $r(x)$. Instead of taking $r(x)$ to be the ℓth cyclotomic polynomial $\Phi_\ell(x)$ with a multiple ℓ of k, we modified the original method by starting from a finite subset of the k-th cyclotomic field $\mathbb{Q}(\zeta_k)$ with a primitive kth root ζ_k of unity so that $r(x)$ can be systematically computable. We use the method of indeterminate coefficients to accomplish our purpose.

As a result, we came up with new families of pairing-friendly curves which will be given explicitly in the poster session. We shall also give explicit numerical results.

References

[1] Brezing, F., Weng, A.: Elliptic curves suitable for pairing based cryptography. Designs, Code and Cryptography **37**(1) (2005) 133–141.

[2] Freeman, D., Scott, M., Teske, E.: A taxonomy of pairing-friendly elliptic curves. Cryptology ePrint Archive: 2006/372 (2006). http://eprint.iacr.org/2006/372/.

[3] Tanaka, S., Nakamula, K.: More constructing pairing-friendly elliptic curves for cryptography. arXiv e-print report 0711.1942. http://arxiv.org/abs/0711.1942.

[4] Tanaka, S., Nakamula, K.: More constructing pairing-friendly elliptic curves for cryptography. Transactions of the Japan Society for Industrial and Applied Mathematics **17**(4) (2007) 595–606. (in Japanese with English abstract).