Relating the Smart-Satoh-Araki and Semaev approaches to the discrete logarithm problem on anomalous elliptic curves

José Felipe Voloch

Very recently it was announced that Semaev [Se], Smart [Sm] and Satoh and Araki [SA] gave a solution of the discrete logarithm problem on elliptic curves over $\mathbf{F}_p$ with p points, p a prime, the so-called anomalous curves. The discrete logarithm problem is to find an procedure so that, given P, Q points on the curve, one finds an integer m with $Q = mP$ or shows that m does not exist. This brief note relates the Smart-Satoh-Araki and Semaev approaches.

Let $E/\mathbf{F}_p$ be an elliptic curve with p points. We need to provide a map $\alpha : E(\mathbf{F}_p) \to \mathbf{Z}/p\mathbf{Z}$. Semaev (see also Rück [R]) proceeds as follows. Fix $P \in E(\mathbf{F}_p), P \neq 0$ and let $\omega = df/f$, where $(f) = p(P - 0)$, so ω is a holomorphic differential. Given $Q \in E(\mathbf{F}_p), Q \neq 0$, find likewise f_Q with divisor $p(Q - 0)$ and define $\alpha(Q) = df_Q/(f_Q\omega)$. The point of the algorithm is that f, f_Q can be computed quickly.

Smart and Satoh and Araki proceed differently. They take a lift $\mathbf{E}$ of E to $\mathbf{Z}/p^2$ and points $\mathbf{P}, \mathbf{Q}$ lifting P, Q. They define $\alpha'(Q) = \lambda(p\mathbf{Q})/\lambda(p\mathbf{P})$, where λ is the elliptic logarithm $\lambda : \mathbf{E}_1 = \ker(\mathbf{E} \to E) \to p\mathbf{Z}/p^2$, provided the expression makes sense (see below). The definition of λ depends on a choice of holomorphic differential $\boldsymbol{\omega}$ on $\mathbf{E}$ and can be computed quickly. According to Tate [T], $\boldsymbol{\omega}$ can be fixed so it lifts ω and so that $exp(\lambda) : \mathbf{E}_1 \to (1 + p\mathbf{Z})/p^2$ is an isomorphism. With this choice of $\boldsymbol{\omega}$, Tate defines $q = exp(\lambda(p\mathbf{P}))$, which is the Serre-Tate parameter ([LST],[K]) in this special case. It follows that $q - 1 = \lambda(p\mathbf{P}) \in p\mathbf{Z}/p^2$ and that $\lambda(p\mathbf{Q}) = (q - 1)n$ if $\mathbf{Q} = n\mathbf{P}$. Therefore, unless $q = 1 \in \mathbf{Z}/p^2$, $\alpha' = \alpha$. This relates the two maps and shows that the method of Smart and Satoh and Araki fails precisely when $q = 1 \in \mathbf{Z}/p^2$, that is, when $\mathbf{E}$ is the canonical lift of E. In the unlikely event this happens they can run their algorithm on another lift and still solve this instance of the discrete logarithm problem.

Acknowledgements: The author would like to thank the NSA (grant MDA904-97-

1-0037) for financial support.

References.

[K] N. M. Katz, *Serre-Tate local moduli*, Springer LNM 868 (1981) 138-202.

[LST] J. Lubin, J-P. Serre and J. Tate, *Elliptic curves and formal groups*, Proc. of the Woods Hole summer institute in algebraic geometry 1964. Unpublished. Available at http://www.ma.utexas.edu/users/voloch/lst.html.

[R] H.-G. Rück, *On the discrete logarithm problem in the divisor class group of curves*, preprint, 1997.

[Se]I. A. Semaev, *Evaluation of discrete logarithms on some elliptic curves*, Math. Comp, to appear.

[Sm] N. Smart, *The discrete logarithm problem on elliptic curves of trace one*, preprint HP-LABS Technical Report (Number HPL-97-128), 1997.

[SA] T. Satoh and K. Araki, *Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves*, preprint, 1997.

[T] J. T. Tate, *Letter to B. Dwork*, November, 15th, 1968.

Dept. of Mathematics, Univ. of Texas, Austin, TX 78712, USA

e-mail: voloch@math.utexas.edu