The discrete logarithm problem on elliptic curves and descents

José Felipe Voloch

The purpose of this note is to relate the discrete logarithm problem (DLP) on elliptic curves to descents and compare our approach to others in the literature. Let G be a group. The DLP for G is to find an procedure so that, given $P, Q \in G$ one finds an integer m with $Q = mP$ or shows that m does not exist. The name discrete logarithm problem comes from the special case where G is the multiplicative group of a finite field. If the DLP on a group is computationally hard then one can use this to construct a cryptosystem ([E],[Ko],[M]). Again the classical case is of the multiplicative group of a finite field but also the group of points on an elliptic curve over a finite field has been considered. The latter is supposed to be harder than the former. Basically there has been two developments in trying to solve the DLP on elliptic curves. First Menezes, Okamoto and Vanstone [MOV] showed that if E is an elliptic curve over $\mathbf{F}_q$ of characteristic p such that p doees not divide $N = \#E(\mathbf{F}_q)$, then DLP on $E(\mathbf{F}_q)$ can be reduced to the DLP on the multiplicative group of an extension of $\mathbf{F}_q$ and, if this extension is of low degree then the DLP on $E(\mathbf{F}_q)$ is as hard as the DLP on $\mathbf{F}_q^*$. This will happen if N has a large factor in common with $q^r - 1$ for some small r. The approach of Menezes, Okamoto and Vanstone has been generalized by Frey and Rück [FR] where it is cast in terms of Tate pairings, but for that they need to lift the curve to a p-adic ring. We will show that this is not necessary and give a simplified version of their approach. Very recently it was announced that Semaev [Se], Smart [S] and Satoh and Araki [SA] gave a solution of the DLP on elliptic curves over $\mathbf{F}_p$ with p points, p a prime. In this note we will recover these results using descents and extend it also to the case where $E(\mathbf{F}_q)$ has a large subgroup of order a power of p, for arbitrary q. For the prime to p case our approach is related to that of Menezes, Okamoto and Vanstone, for the p-part it is related to Semaev's (see also Rück [R]) but is very different from Smart's and Satoh and Araki's, although we will study the relation between these approaches also. The unifying theme of our approach is the old technique of descents on elliptic curves.

Let $\phi : E' \to E$ be an isogeny of elliptic curves defined over a field k. The exact sequence $0 \to \ker\phi \to E' \to E \to 0$ yields by taking flat (or Galois, if ϕ is separable) cohomology, an injection $E(k)/\phi(E'(k)) \to H^1(k, \ker\phi)$. For instance we could take ϕ to be $1 - F$, F the $\mathbf{F}_q$-Frobenius, if $E = E'$ is defined over $\mathbf{F}_q$ and we get an injection of $E(\mathbf{F}_q)$ into $H^1(\mathbf{F}_q, \ker\phi)$ and in theory we can reduce the problem to the DLP on the latter group.

In practice, we need to be a bit more careful. Let us assume that $E(\mathbf{F}_q)$ is cyclic. This is the most interesting case for cryptographic applications and also if E is any ordinary elliptic curve then it is isogenous to one that has a cyclic group of rational points ([V1], lemma 1). Let N be the number of rational points on E and let us write $N = p^m n$ with $(n, p) = 1$. One can construct an isogeny $\phi : E' \to E$, for some $E'/\mathbf{F}_q$ such that $E(\mathbf{F}_q)/\phi(E'(\mathbf{F}_q))$ is of order n and moreover we can assume that $\ker\phi$ is cyclic of order n. A similar construction is done in [V2]. If the points of $\ker\phi$ are defined over $\mathbf{F}_{q^r}$ then the relevant cohomology group injects into $\mathbf{F}_{q^r}^*/(\mathbf{F}_{q^r}^*)^n$. The latter group is isomorphic to the n-th roots of unity by $x \mapsto x^{(q^r-1)/n}$ and from this isomorphism one recovers the original approach of [MOV]. A similar calculation is done in [H]. Whether working on $\mathbf{F}_{q^r}^*/(\mathbf{F}_{q^r}^*)^n$ or the n-th roots of unity is better computationally is unclear. The map $E(\mathbf{F}_q)/\phi(E'(\mathbf{F}_q)) \to \mathbf{F}_{q^r}^*/(\mathbf{F}_{q^r}^*)^n$ can be given explicitly as $P \mapsto f(P) \pmod{(\mathbf{F}_{q^r}^*)^n}$ for a suitable function f on E (see e.g. [Si], thm. X.1.1 and ex. 10.9). Computing f can be done following Miller's algorithm described on [MOV], appendix A. As mentioned above this is essentially the approach of [MOV] for the prime-to-p part. We turn to the p-part.

Again let N be the number of rational points on E and let us write $N = p^m n$ with $(n, p) = 1$. We assume that $m > 0$, so E is ordinary. Let $E^{(p^m)}$ be the image of E under the m-th power of the Frobenius map F^m and $V_m : E^{(p^m)} \to E$ the dual isogeny, the m-th order Verschiebung, which is separable since E is ordinary. By our assumption, the p^m-torsion points on E are defined over $\mathbf{F}_q$, so the same is true for $E^{(p^m)}$. We thus get an injective descent map $\alpha : E(\mathbf{F}_q)/V_m(E^{(p^m)}(\mathbf{F}_q)) \to W_m(\mathbf{F}_q)/\wp(W_m(\mathbf{F}_q))$, where $W_m(\mathbf{F}_q)$ is the ring of Witt vectors of lenght m over $\mathbf{F}_q$, $\wp$ is the map $x \mapsto Fx - x$, where F is the

Frobenius on $W_m(\mathbf{F}_q)$ and the cohomology group is as stated because of Artin-Schreier-Witt theory. Also, if we denote by $T : W_m(\mathbf{F}_q) \to W_m(\mathbf{F}_p) \cong \mathbf{Z}/p^m\mathbf{Z}$ the trace map, then $W_m(\mathbf{F}_q)/\wp(W_m(\mathbf{F}_q))$ is mapped isomorphically onto $W_m(\mathbf{F}_p) \cong \mathbf{Z}/p^m\mathbf{Z}$ by T, by the additive form of Hilbert's theorem 90. We have thus reduced the DLP on the p-part of $E(\mathbf{F}_q)$ to the DLP on $\mathbf{Z}/p^m\mathbf{Z}$ which is, of course, trivial. The only remaining question in this case is the explicit calculation of the map α above.

Let us look at a special case corresponding to the work by Smart et al. mentioned above. Assume then that $q = p = N$ so we need to provide a map $\alpha : E(\mathbf{F}_p) \to \mathbf{Z}/p\mathbf{Z}$. Assume $p \neq 2$. Choose a Weierstrass equation $y^2 = x^3 + a_2x^2 + a_4x + a_6 = f(x)$ for E. Define polynomials U, M , with $\deg U \leq p-2$ by $y^{p-1} = f(x)^{(p-1)/2} = U(x) + Ax^{p-1} + x^pM(x)$. (Note that A is the Hasse invariant and, in our case, in fact $A = 1$.) Then $\alpha(x, y)$ is simply $yM(x)$ ([V3], proposition 1.3). More generally, if $m = 1$ above, the map is $\alpha(x, y) = T(yM(x))$, which also follows from the same result on [V3]. For the case of general m we have:

Theorem. *Let $E/\mathbf{F}_q$ be an elliptic curve given by a generalized Weierstrass equation $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$. There exists $r_0, \ldots, r_{m-1} \in \mathbf{F}_q[x, y]$ satisfying $\deg r_i \leq 2^ip^{i+1}$ such that $T \circ \alpha : E(\mathbf{F}_q) \to W_m(\mathbf{F}_p) = \mathbf{Z}/p^m\mathbf{Z}$ is given by $P \mapsto T((r_0(P), \ldots, r_{m-1}(P)))$.*

Proof: The elliptic curve E has a canonical lifting to an elliptic curve $\mathbf{E}$ over $W_m(\mathbf{F}_q)$ for which the Frobenius $E \to E^{(p)}$ also lifts. This is a special case of the Serre-Tate theory (see [LST] or [K]). There is also an injective homomorphism $\tau : E(\bar{\mathbf{F}}_q) \to \mathbf{E}(W_m(\bar{\mathbf{F}}_q))$ compatible with the action of Frobenius, which we will call the elliptic Teichmüller lift (see [Bu] or [VW]). In fact, a characterization of the canonical lift is the existence of such a homomorphism. Likewise $E^{(p^m)}$ has a lift $\mathbf{E}'$ which is the image of $\mathbf{E}$ by the m-th power of the lift of Frobenius. Fix a holomorphic differential ω on $\mathbf{E}'$.

There exists an unique function ζ on $\mathbf{E}'/W_m(\mathbf{F}_q)$ which is odd, has simple poles at the points of $G = \tau(\ker V_m)$ and no others and $\operatorname{res}(\zeta\omega) = 1$ at these points. This uniquely

characterizes ζ. This implies that if P_1 is in G then $\zeta(P+P_1) = \zeta(P) + c(P_1)$ where $c(P_1) \in W_m(\mathbf{F}_q)$ and this gives a homomorphism $c : G \to W_m(\mathbf{F}_q)$. We can write $\zeta(t(P))$ as a Witt vector $(z_0(P), ..., z_{n-1}(P))$ where the z_i are functions on $E^{(p^m)}$. It follows from the above that $Z = (z_0, ..., z_{m-1})$ satisfies an equation $F(Z) - AZ = R \in W_m(\mathbf{F}_q(E))$ for some $A \in W_m(\mathbf{F}_q)$. Since $\mathbf{F}_q(E^{(p^n)})/\mathbf{F}_q(E)$ is an Artin-Schreier-Witt extension, we must have $A = 1$ after scaling. It follows then that $P \mapsto R(P)$ gives the descent map, just as in the case $m = 1$. To get the bound on the degrees of the coordinates of R, we use theorem 4.1 of [VW]. Since ζ has degree p^m, it implies that the z_i have degree at most $(2p)^i p^m$ as functions on $E^{(p^n)}$. So the r_i have degree at most $(2p)^i p^{m+1}$ as functions on $E^{(p^n)}$ but this means that they have degree at most $(2p)^i p$ as functions on E, since V_m has degree p^m. This completes the proof.

We will now compare our approach to the other 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.

To relate Semaev's map to the one we defined previously, consider the function $\zeta = z_0$ from the proof of the theorem when $m = 1$. As proved in ([V4],pg. 4), Semaev's α satisfies $\alpha(Q) = -\eta(Q)$, where $\eta(Q) = \zeta(R + Q) - \zeta(R)$, for generic R. Now, as in the proof of the theorem, $\zeta^p - \zeta = yM(x) \circ V_1$. Choose now a point T on E with $V_1(T) = Q$ then, for our previously defined α, $\alpha(Q) = yM(x)(Q) = z(T)^p - z(T) = z(F(T)) - F(T) = z(T + F(T) - T) - z(T) = \eta(F(T) - T)$, where F is the Frobenius. It is enough now to show that $F(T) - T = -Q$. Notice however that, since E has p points over $\mathbf{F}_p$, F satsifies the equation $F^2 - F + p = 0$ and $F \equiv 1 \pmod p$. This implies that $F \equiv 1 - p \pmod{p^2}$ and, since $p^2T = 0$ we get $F(T) - T = (1-p)T - T = -pT = -F(V_1(T)) = -F(Q) = -Q$.

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 $\alpha'(Q) = l(p\mathbf{Q})/l(p\mathbf{P})$, where l is the elliptic

logarithm $l : \mathbf{E}_1 = \ker(\mathbf{E} \to E) \to p\mathbf{Z}/p^2$, provided the expression makes sense (see below). The definition of l depends on a choice of holomorphic differential ω on $\mathbf{E}$ and can be computed quickly. According to Tate [T], ω can be fixed so it lifts ω and so that $\exp(l) : \mathbf{E}_1 \to (1 + p\mathbf{Z})/p^2$ is an isomorphism. With this choice of ω, Tate defines $q = \exp(l(p\mathbf{P}))$, which is the Serre-Tate parameter ([LST],[K]) in this special case. It follows that $q - 1 = l(p\mathbf{P}) \in p\mathbf{Z}/p^2$ and that $l(p\mathbf{Q}) = (q-1)n$ 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.

[Bu] A. Buium, *An approximation property for Teichmüller points*, Math. Research Letters, **3** (1996) 453–457.

[E] T. ElGamal,*A public key cryptosystem and a signature scheme based on discrete logarithms*, Advances in Cryptology - Proceedings of CRYPTO'84, Springer Verlag Lecture Notes in Computer Science vol. 196, 1985, pp 10-18.

[H] E. Howe, *The Weil pairing and the Hilbert symbol*, Math. Annalen, **305** (1996), 387–392.

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

[Ko] N. Koblitz, *Elliptic curve cryptosystems*, Math. of Computations, **48**(1987), 203-209.

[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.

[M] V.S. Miller, *Use of elliptic curves in cryptography*, Advances in Cryptology - Proceedings of CRYPTO'85, Springer Verlag Lecture Notes in Computer Science vol. 218, 1986, pp 417-426.

[MOV] A. Menezes, T. Okamoto and S. Vanstone *Reducing elliptic curves logarithms to logarithms in a finite field*, IEEE Trans. Info. Theory,**39**, (1993) 1639-1646.

[R] H.-G. Rück, *On the discrete logarithm problem in the divisor class group of curves*, Math. Comp., to appear.

[Se] I. A. Semaev, *Evaluation of discrete logarithms on some elliptic curves*, Math. Comp., **67** (1998), 353–356.

[Si] J. H. Silverman, *The arithmetic of elliptic curves*, Springer, New York, 1986.

[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*, Comment. Math. Univ. St. Paul. **47** (1998), 81–92.

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

[V1] J. F. Voloch, *A note on elliptic curves over finite fields.* Bull. Soc. Math. France **116**(1988), 455-458.

[V2] J. F. Voloch, *Primitive points on constant elliptic curves over function fields.* Bol. Soc. Brasil. Mat.**21**(1990), 91-94.

[V3] J. F. Voloch, *Explicit p-descent for elliptic curves in characteristic p*, Compositio Math. **74** (1990) 247-258.

[V4] J. F. Voloch, *An analogue of the Weierstrass ζ-function in characteristic p*, Acta Arithmetica, **LXXIX** (1997) 1-6.

[VW] J. F. Voloch and J. L. Walker, *Euclidean weights of codes from elliptic curves over rings*, preprint, 1997.

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

e-mail: voloch@math.utexas.edu