Elliptic Curves in Cryptography

Ian Blake, Gadiel Seroussi and Nigel Smart

Errata

(for first and second printings[1])

p. 7: Line 6 should read 'finite fields and a finite number of abelian varieties. For all practical purposes, the latter can be taken to be Jacobians of curves.'

p. 7: Line -3. Insert 'some of' after 'breaking'.

p. 14: Step 6 of Algorithm II.2 (Barrett Reduction) should be

$$6.\ \texttt{While}\ z \geq p\ \ \texttt{do}\ z \leftarrow z - p.$$

p. 42: Line 6 should read

$$Y^2 + XY = X^3 + a_2X^2 + a_6.$$

p. 57: Line -1 should read

$$y_3 = (x_1 - x_3)\lambda - y_1.$$

p. 58: Line 4 should read

$$y_3 = (x_1 - x_3)\lambda - y_1.$$

p. 76: Line -12 should read 'So, m can be 'divided' by $\varphi^n - 1$ ...'

p. 89: Replace the first full paragraph with the following.

Let E denote an elliptic curve defined over the field of p-adic numbers, $\mathbb{Q}_p$, which is assumed to have good reduction at p. The set of points of $E(\mathbb{Q}_p)$ which reduce to zero modulo p is denoted by $E_1(\mathbb{Q}_p)$ which is a group. The set of points in $E(\mathbb{Q}_p)$ which reduce modulo p to an element of $E(\mathbb{F}_p)$ is denoted by $E_0(\mathbb{Q}_p)$. In our case of E having good reduction at p we have $E(\mathbb{Q}_p) = E_0(\mathbb{Q}_p)$ but to remain consistent with the more general literature we shall still retain the notation $E_0(\mathbb{Q}_p)$. There is the exact sequence

pp. 92–97: Rho, lambda and kangaroo methods. Although the method described in Section V.5 is similar to schemes recently used in practical attacks on the ECDLP, our discussion of the rho, lambda and kangaroo methods does not accurately reflect their original descriptions. The following corrections are intended to clarify the differences between the methods and reduce confusion.

[1]These errata have been corrected in the third printing of June 2000.

p. 92: Replace the paragraph before the start of the example with the following.

The rho and lambda methods, discussed in more detail in the next subsection, also have complexity $O(\sqrt{n})$. The time to sort and search the look-up table in the BSGS method can be eliminated if a hash table is used instead. In this case, the constant multiplying $\sqrt{n}$ in the asymptotic estimate can be made $\frac{4}{3}$. Pollard's rho method has a slightly better constant, roughly $\frac{5}{4}$. However, this is only an *expected* running time, given the randomized nature of the method. The lambda method, on the other hand, has a constant of 2, again applied to expected running time. The advantage of the rho and lambda methods is that their storage requirements can be made arbitrarily small.

p. 93: Section V.5. Change the title to **'Methods based on Random Walks'**.

Replace the first two paragraphs of the section with the following.

Pollard [**125**] gives a number of methods to solve the discrete logarithm problem in a variety of groups. The rho method uses a single random walk and waits for a cycle to occur. By using a space-efficient method to detect the cycle, the discrete logarithm can be found. The wait for the cycle means that the single random walk can be thought of as tracing out the greek letter rho, ρ.

In Pollard's lambda method (often called the method of tame and wild kangaroos), two random walks are used, one by a tame kangaroo who jumps off into the wild, digs a hole and waits for the wild kangaroo to fall into it. The two paths form the shape of the greek letter lambda, λ. The lambda method is suited to finding discrete logarithms which are known to lie in a short interval.

There is a parallel version of the rho method, which uses many random walks. However, despite the method's name, the 'paths' do not now look like a rho, since instead one looks for two paths that intersect. The method described in this section is what is usually referred to as the parallel rho method.

The following intuitive explanation uses the analogy of jumping animals, since we have found this to be useful when explaining the method in lectures. However, these are not the kangaroos of Pollard's method, since Pollard's kangaroos perform better controlled jumps. We shall call our jumping animals 'snarks', since they jump around in a rather uncontrolled manner.

p. 94: First paragraph should be replaced with the following.

To simplify the matter we take two snarks. Eventually we shall use a larger number of snarks. The two snarks are given a spade and told that they should dig a hole every ten or so jumps. Where each snark jumps next depends on the position they are currently at, hence

when one snark meets the path of the other (or itself) it will follow the original path along until it falls into one of the holes that have been dug.

pp. 94–96: Replace 'kangaroo' with 'snark' throughout. Remove references to 'tame' and 'wild' snarks, since all snarks are 'wild'.

p. 95: Line 17. Remove ', which gives the method one of its names.'

p. 97: Line -17. Remove the word 'small'.

p. 98: Line -6 should read 'the other supersingular curves.'

p. 104: Line -7. Replace 'can be significantly diminished' with 'can be made arbitrarily small.'

p. 112: Line -5 (of the main text). The inequality should be an equality.

p. 114: Footnote. Insert comma after 'comments'.

p. 171: Line -11. The sum should run over $P \in C(\overline{\mathbb{F}}_q)$.

p. 176: Line 10. Remove ', what is no surprise,'.

p. 193: In reference [37], the author is R. Crand*a*ll.

pp. 191–198: The following references have now appeared.

[89] *JLMS*, Vol 59, pp 448-460, 1999.
[118] *Math. Comp.*, Vol 68, pp 1233-1241, 1999.
[152] *J. Cryptology*, Vol 12, pp 141-151, 1999.
[153] *J. Cryptology*, Vol 12, pp 193-196, 1999.