Generating Anomalous Elliptic Curves - Erratum

Franck Leprévost [a], Jean Monnerat [b,1], Sébastien Varrette [a], Serge Vaudenay [b]

[a] *Université du Luxembourg, LIASIT, 162 A, Avenue de la Faïencerie, L-1511 Luxembourg*

[b] *EPFL, LASEC, CH-1015 Lausanne, Switzerland*

This document provides an erratum of the article "Generating Anomalous Elliptic Curves" which was published in *Information Processing Letters*, vol. 93, pp. 225-230, Elsevier, 2005. At page 229, a mistake occured in the curve given in Example 1. A digit is missing in the coefficient μ which leads to a non-anomalous curve. Below, we rewrite Example 1 correctly with right coefficients as well as new points P and Q of the curve.

Example 1. For $m = 257743850762632419871495$, $p = 11m(m+1) + 3$ is a prime number of length 160 bits. Then, the elliptic curve E over $\mathbf{F}_p$ is defined by the equation $y^2 = x^3 + \mu x + \nu$, where

$$\mu = 425706413842211054102700238164133538302169176474,$$

and

$$\nu = 203362936548826936673264444982866339953265530166,$$

and one checks that $E(\mathbf{F}_p) = p$, and the curve E is anomalous over $\mathbf{F}_p$. Now, if

$$P = (13, 46554427381428317095586081497956690905883952130\,5) \in E(\mathbf{F}_p)$$

and

$$Q = (17, 173827014976148521051073746232750578872372755801) \in E(\mathbf{F}_p),$$

Email addresses: `Franck.Leprevost@univ.lu` (Franck Leprévost), `Jean.Monnerat@epfl.ch` (Jean Monnerat), `Sebastien.Varrette@imag.fr` (Sébastien Varrette), `Serge.Vaudenay@epfl.ch` (Serge Vaudenay).

[1] Supported in part by a grant of the Swiss National Science Foundation, 200021-101453/1.

the method shows that $Q = nP$, with

$$n = 615421018442001462563539981905852134696556435295.$$

Acknowledgements. The authors would like to thank Jan steffen Müller for pointing out this mistake.