Elliptic Curves in Cryptography

Ian Blake, Gadiel Seroussi and Nigel Smart

Errata

(for second edition and printings of June 2000 and later)

p. 9: The formula for $C_{\mathrm{CONV}}(N)$ has a $\log 2$ missing. It should read

$$C_{\mathrm{CONV}}(N) = \exp\left(c_0 \, (N \log 2)^{1/3} \, (\log(N \log 2))^{2/3} \right).$$

p. 47: Line -1. Replace "$a = -g_2/\sqrt[3]{4}$, $b = -g_3$" with "$a = -g_2/4$, $b = -g_3/4$".

p. 54: Line 11. Replace "for $i = 1, ..., \ell{+}1$" should be "for $r = 1, ..., \ell{+}1$".