Erratum


Page 183, line 4, should read:
\[ f(x) = A + T(ux) + \sum_{i=1}^{h} T(\beta_i x) T(\gamma_i x) \mod x^{2^{m-1}} + 1, \] (1)

Page 183, lines 12 and 13, should read:
\[ f'(x) = u + \sum_{i=1}^{h} (\beta_i T(\gamma_i x) + \gamma_i T(\beta_i x) + (\beta_i \gamma_i)^{2^{m-1}}) \]
\[ = u + \sum_{i=1}^{h} (\beta_i \gamma_i)^{2^{m-1}} + L(x), \]

Page 184, line 11, should read:
\[ Q(y) = T(y^3 + y^5 + y^9 + \cdots + y^{1+2^{(m-1)/2}}) \mod y^{2^{m-1}} + 1. \]