Consturction of Algebraic Error Control Codes on the Elliptic Riemann Surface

M.Hassner†, W. Burge, S. M. Watt††

Abstract:

In this paper we make use of the power series facility of Scratchpad2, a symbolic computer language under development at the IBM Research Mathematics Department, to construct algebraic ECC on the elliptic Riemann surface of genus one. The construction method described uses products of elliptic theta series with rational characteristics and finite field coefficients to define the projective coordinates of normal finite field elliptic curves. The curve equations are identities satisfied by these power series. Their order is the common denominator of the rational theta characteristics. The rational points on the curve which are used to locate the symbols inside a codeword correspond in a one to-one-one manner with the points on the grid obtained by the appropriate rational division of the elliptic period rectangle. At these points the projective coordinate ratios in our curve description are modular forms given as q-series,where q is the nome. We apply Pade approximation to these q-series and obtain rational approximants.These approximants satisfy the curve equation and constitute our computational model.We demonstrate its usefulness by constructing codes on the normal elliptic cubic and quintic.

† IBM Research Division, Almaden Research Center, San Jose, California 95120-6099

†† IBM Thomas J. Watson Research Center, Box 218 Yorktown Heights,New York 10598