The ECDONALD BAT

Daniel J. Bernstein *

djb@cr.yp.to

ECDONALD is just like DONALD but uses ECDSA instead of DSA. It supports the 15 NIST curves and one additional curve, `secp160r1`.

* Date of this document: 2007.02.13.