binary.cr.yp.to

D. J. Bernstein
University of Illinois at Chicago

NSF ITR–0716498

2003 Rodríguez-Henríquez–Koç,
2005 Chang–Kim–Park–Lim,
2006 Weimerskirch–Paar,
2006 von zur Gathen–Shokrollahi,
2007 Peter–Langendörfer:
minimizing bit operations
for poly mult mod 2,
using Karatsuba etc.

binary.cr.yp.to/m.html:
even fewer bit operations.
Has been used in new ECC
software speed records.
Maybe useful for hardware!

binary.cr.yp.to
/linearmod2.html:
new paper describing
algorithm to compile
any linear map mod 2
into a series of xors.

Compiled code is efficient:
e.g. 922 ± 8 xors for
random 64-bit-to-64-bit map.
Often competitive with
ad-hoc optimization.

Compilation algorithm is
fast, surprisingly simple.