John Black
Dept. of Computer Science
430 UCB
University of Colorado
Boulder, CO 80309 USA

jrblack@cs.colorado.edu
www.cs.colorado.edu/~jrblack

Phillip Rogaway
Dept. of Computer Science
University of California
Davis, CA 95616 USA **and**
Dept. of Computer Science
Faculty of Science
Chiang Mai University
Chiang Mai 50200 Thailand
rogaway@cs.ucdavis.edu
www.cs.ucdavis.edu/~rogaway

12 May 2003

William Burr
Morris Dworkin
Security Technology Group
National Institute of Standards and Technology
Computer Security Division
william.burr@nist.gov
morris.dworkin@nist.gov

Dear NIST:

This letter is to reiterate that neither of us holds any patents or pending patents that cover XCBC or OMAC, and neither of us is aware of any patents or pending patents relevant to these algorithms. Our own work on XCBC (including any follow-up work on that algorithm that we played a role in) has been placed in the public domain. As far as we know, XCBC and OMAC are free and unencumbered for all uses.

Sincerely,

John Black *and*
Phillip Rogaway