Department of
Computer Science

SECOND READER FORM

FOR

THESIS OR TWO SEMESTER WORK

Name: Katherine Ye **Class:** 2016

Senior Thesis 2nd Reader Prof. Matt Green (Johns Hopkins) (matthewdgreen@gmail.com)

Title of project (Please Print Clearly): Formally proving cryptographic security of a pseudo-random number generator

Short description of project: I will complete computer-checked proofs of security properties of the widely-used pseudo-random number generator HMAC-DRBG. Specifically, I will prove that its output is indistinguishable from random and that its design is backtracking-resistant.

Return this **signed** form to Colleen Kenny-McGinley in Room 210, no later than the deadline (see course website for deadline).

I agree to be a 2nd reader (*signature needed for senior thesis or two semester IW only)*

FACULTY SIGNATURE **FACULTY NAME & DEPARTMENT**