998-68-44 **Adam L Young*** (ayoung@cigital.com), 21351 Ridgetop Circle, Suite 400, Dulles, VA 20166, and **Moti M Yung** (moti@cs.columbia.edu), Room 464, S. W. Mudd Building, Computer Science Dept., Columbia University, New York, NY 10027. *A Key Recovery System as Secure as Factoring.*

There has been a lot of recent work in the area of proving in zero-knowledge that an RSA modulus N has the correct form. For example, protocols have been given that prove that N is the product of: two safe primes, two primes nearly equal in size, etc. Such proof systems are rather remarkable in what they achieve, but may be regarded as being heavyweight protocols due to the computational and messaging overhead they impose. In this paper an efficient zero-knowledge protocol is given that simultaneously proves that N is a Blum integer and that its factorization is recoverable by a designated key recovery authority. The protocol assumes the availability of a semantically secure encryption function. The solution is therefore amenable for use with systems based on PKCS #1. A proof is given that shows that our algorithm is secure under the integer factorization problem (and can be turned into a non-interactive zero-knowledge proof in the random oracle model). The result appears in CT-RSA '04. (Received January 05, 2004)