

# Cryptology ePrint Archive: Report 2011/612

## IBAKE: Identity-Based Authenticated Key Exchange Protocol

*Vladimir Kolesnikov and Ganapathy S. Sundaram*

**Abstract:** The past decade has witnessed a surge in exploration of cryptographic concepts based on pairings over Elliptic Curves. In particular, identity-based cryptographic protocols have received a lot of attention, motivated mainly by the desire to eliminate the need for large-scale public key infrastructure.

We follow this trend in this work, by introducing a new Identity-Based Authenticated Key Exchange (IBAKE) protocol, and providing its formal proof of security. IBAKE provides mutually-authenticated Key Exchange (AKE) using identities as public credentials.

One identity-based AKE subtlety that we address in this work is the resilience to the man-in-the-middle attacks by the Key Management Service. For efficiency, we employ two Elliptic Curves with differing properties. Specifically, we use a combination of a super-singular and non-super-singular curves, where the super-singular curve is used as an identity-based encryption "wrapper" to achieve mutual authentication, and the resulting session key is based on a Diffie-Hellman key exchange in the non-super-singular curve.

We provide a detailed proof of security of the resulting protocol with respect to (our own natural adaptation and simplification of) the AKE definitions of Kolesnikov and Rackoff.

**Category / Keywords:** cryptographic protocols / Identity-based Authenticated Key Exchange

**Date:** received 11 Nov 2011

**Contact author:** kolesnikov at research bell-labs com

**Available formats:** [PDF](#) | [BibTeX Citation](#)

**Version:** 20111115:175045 ([All versions of this report](#))

**Discussion forum:** [Show discussion](#) | [Start new discussion](#)

---

[ [Cryptology ePrint archive](#) ]