Cryptology ePrint Archive: Report 2012/732

Non-Interactive Key Exchange

Eduarda S.V. Freire and Dennis Hofheinz and Eike Kiltz and Kenneth G. Paterson

Abstract: Non-interactive key exchange (NIKE) is a fundamental but much-overlooked cryptographic primitive. It appears as a major contribution in the ground-breaking paper of Diffie and Hellman, but NIKE has remained largely unstudied since then. In this paper, we provide different security models for this primitive and explore the relationships between them. We then give constructions for secure NIKE in the Random Oracle Model based on the hardness of factoring and in the standard model based on the hardness of a variant of the decisional Bilinear Diffie Hellman Problem for asymmetric pairings. We also study the relationship between NIKE and public key encryption (PKE), showing that a secure NIKE scheme can be generically converted into an IND-CCA secure PKE scheme. This conversion also illustrates the fundamental nature of NIKE in public key cryptography.

Category / Keywords: cryptographic protocols /

Publication Info: This is the full version of a paper to appear at PKC 2013

Date: received 31 Dec 2012

Contact author: kenny paterson at rhul ac uk

Available formats: PDF | BibTeX Citation

Version: 20130101:143205 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]