Computational Science and Its Applications-ICCSA 2010
6019: 225-235

A Novel Convinced Diffie-Hellman Computation Scheme and Its Cryptographic Application

Tseng, Yuh-Min; Wu, T. Y.

Abstract

The Diffie-Hellman (DH) problem is an important security assumption in modern cryptography. In this paper, a new type of cryptographic technique called a convinced Diffie-Hellman (DH) computation scheme is proposed. In the convinced DH computation scheme, an issuer can convince a verifier that the computation of the Diffie-Hellman problem is correct under without revealing any exponential parts of two Diffie-Hellman public values. Firstly, the formal framework and security requirements for this new cryptographic scheme are defined. Then a concrete scheme is proposed. In the random oracle model and under the difficulty of computing discrete logarithm, we demonstrate that the proposed scheme meets the defined security requirements. Finally, we present an important application of the convinced DH computation scheme. Most group key agreement protocols provide only the functionality of detecting the existence of malicious participants, but don’t identify who malicious participants are. The novel convinced DH computation scheme can be embedded in many multi-round group key agreement protocols to identify malicious participants and provide fault tolerance.

Key words：Diffie-Hellman problem; Convinced computation; Malicious participant; Group key agreement; Cryptography