DAVID JAO, University of Waterloo

Boneh–Boyen signatures and the Strong Diffie–Hellman problem

The recent advent of non-standard discrete logarithm based assumptions has led to a proliferation of cryptographic protocols for which no proof of equivalence between the security of the protocol and the underlying hard problem is known. One of the prototypical examples of this phenomenon is the Boneh–Boyen short signature scheme, whose security to date has not been proven to be equivalent to the Strong Diffie–Hellman (SDH) problem upon which it is based. The results which we present here provide for the first time a proof that the Boneh–Boyen signature scheme is equivalent to the SDH problem. Using Cheon's algorithm for solving the SDH problem, we obtain an algorithm that in most cases recovers the private key in the Boneh–Boyen signature scheme in less time than it takes to solve the discrete logarithm problem, given sufficiently many message-signature pairs.