# The development of deniable authentication protocol based on the bivariate function hard problem

## ABSTRACT

A deniable authentication protocol enables a receiver to identify the true source of a given message but not to prove the identity of the sender to the third party. Non-interactive protocol is more efficient than interactive protocol in terms of communication overhead, and thus several non-interactive deniable authentication protocols have been proposed. So, it is very necessary to design a deniable authentication protocol which is non-interactive, secure and efficient. This paper proposes a deniable authentication protocol based on the bivariate function hard problem (BFHP) cryptographic primitive. An improvement based on the BFHP is suggested since the problem of the BFHP provides the needed security elements plus its fast execution time. At the same time, the proposed protocol has properties of completeness, deniability, security of forgery attack, security of impersonation attack and security man-in-the-middle attack also has been proved.