

**CHENNAI – PONDICHERRY**

**PROVABLY SECURE DYNAMIC ID-BASED ANONYMOUS TWO-FACTOR AUTHENTICATED KEY EXCHANGE PROTOCOL WITH**

**EXTENDED SECURITY MODEL**

**Abstract:**

Authenticated key exchange (AKE) protocol allows a user and a server to authenticate each other and generate a session key for the subsequent communications. With the rapid development of low-power and highly-efficient networks, such as pervasive and mobile computing network in recent years, many efficient AKE protocols have been proposed to achieve user privacy and authentication in the communications. Besides secure session key establishment, those AKE protocols offer some other useful functionalities, such as two-factor user authentication and mutual authentication. However, most of them have one or more weaknesses, such as vulnerability against lost-smart-card attack, offline dictionary attack, de-synchronization attack, or the lack of forward secrecy, and user anonymity or untraceability. Furthermore, an AKE scheme under the public key infrastructure may not be suitable for light-weight computational devices, and the security model of AKE does not capture user anonymity and resist lost-smart-card attack. In this paper, we propose a novel dynamic ID-based anonymous two-factor AKE protocol, which addresses all the above issues. Our protocol also supports smart card revocation and password update without centralized storage. Further, we extend the security model of AKE to support user anonymity and resist lost-smart-card attack, and the proposed scheme is provably secure in extended security model. The low-computational and bandwidth cost indicates that our protocol can be deployed for pervasive computing applications and mobile communications in practice.