

十一、研究計畫中英文摘要：請就本計畫要點作一概述，並依本計畫性質自訂關鍵詞。

(二) 計畫英文摘要。(五百字以內)

Along with the popularization of third generation mobile communication system (3G), more and more people enjoy the living type of using network at anywhere and anytime. The 3G network system provides the functions of real-time messages, multi-media conferencing, digital data sharing and interactive games. The identity management of 3G mobile network systems cannot to be neglected and the 3G mobile network system identity management, that it manages the identity and access control of users. The major purpose is to prevent the illegal user impersonate to service, prevent personal information stole and prevent any kind of attacks. Thus, the 3G needs an integrity authentication protocol and the protocol must be established between 3G network users and 3G network provider, which can resist the third party attack of the verify and authorize messages. Otherwise, the cost of the message communication between VLR and HLR is very expensive, especially when VLR and HLR are located in different countries. Our proposed scheme is based on the agency scheme, and the VLR just need to ask HLR to get agency key at the first time. The VLR can use the pre-agency key to authenticate the user when the user is in the foreign or specific area. If the user moves to other new VLR area and the new VLR just need to ask pre-VLR to get the agency key in the same network.

Keywords: Authentication, information security, the third generation mobile communication, Universal Mobile Telecommunications System (UMTS).