doi:10.1631/FITEE.1400232

题目：一套具备使用者不可追踪性的轻量化身分鉴别机制

目的：随着电子商务应用的蓬勃发展，如何安全且有效率地提供足够的网路资源或线上服务给远端使用者逐渐成为一门研究显学。鉴于此，本论文主要针对目前商务网路环境设计使用者身分鉴别机制。

创新点：本研究所提出的鉴别机制主要利用杂凑函数(Hash function)作为机制内的资讯保护技术，并以一套新设计的讯息传递逻辑成功完成多个体间的相互身分鉴别，如此将可同时达到计算安全与轻量化效能两大效益。

方法：藉由使用者注册(Registration)、登入与鉴别(Login and authentication)、密码变更(Password change)等三大阶段来完成并良好管理使用者身分鉴别与讯息传输安全。

结论：本论文主要针对现有网路环境下的商务架构，进行使用者身分鉴别机制设计。在协定安全度方面，根据传输逻辑分析与安全正式化分析结果，所提方法的安全可行性已被成功证实。在效能方面，本研究比近期所提出的几份相关机制(Tsai *et al.*, 2013；Chang *et al.*, 2014；Kumari and Khan, 2014)皆更为有效率（表 2、3）。

关键词：身分鉴别；隐私；安全；智慧卡；不可追踪性