Abstract:

Usual password schemes suffer from the flaw that they are easy to steal. An attacker who has correctly observed a login session (by peeping, wiretapping and/or by launching a "man-in-the-middle" attack, etc.) can easily impersonate the corresponding user. Available protection techniques require computations on hundreds digit integers that are so complex that they require special software and/or hardware. This project tries to combine the simplicity of the conventional password schemes with a protection technique that results in a different password being typed each session, but only requires simple computation performed in the user's head.