

Cryptology ePrint Archive: Report 2011/359

High-Entropy Visual Identification for Touch Screen Devices

Nathaniel Wesley Filardo and Giuseppe Ateniese

Abstract: We exhibit a system for improving the quality of user-derived keying material on touch-screen devices. We allow a device to recover previously generated, highly entropic data suitable for use as (part of) a strong secret key from a user's act of identifying to the device. Our system uses visual cryptography [22], using no additional electronics and no memorization on the part of the user. Instead, we require the use of a transparency overlaid on the touch-screen. Our scheme is similar to the identification scheme of [23] but tailored for constrained, touch-screen displays.

Category / Keywords: applications / visual cryptography, user identification

Date: received 4 Jul 2011

Contact author: nwf at cs jhu edu

Available formats: [PDF](#) | [BibTeX Citation](#)

Version: 20110706:024357 ([All versions of this report](#))

Discussion forum: [Show discussion](#) | [Start new discussion](#)

[[Cryptology ePrint archive](#)]