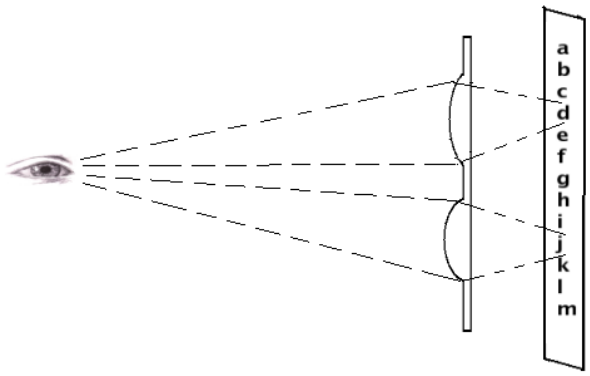
Eberhard Karls Universität Tübingen
Wilhelm-Schickard-Institut für Informatik (WSI)
**Arbeitsbereich für Theoretische Informatik/Formale Sprachen**

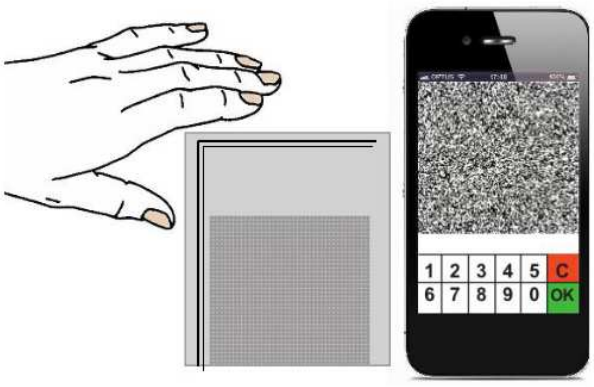
**Thema für eine Master- oder Diplomarbeit** 12. März. 2013

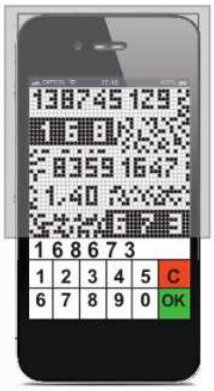
# Sicherheitsanalyse zur Mehrfach-Verwendbarkeit der Lichtbrechungs-Kryptographie

Es soll eine neue Variante der Visuellen Kryptographie untersucht werden, bei der nicht mit Folien mit aufgedruckten Pixeln, die sich beim Übereinanderlegen der Folien überdecken oder nicht, gearbeitet wird, sondern mit durchsichtigen Karten mit kleinen Prismen und/oder Linsen, durch die die Lichtstrahlen umgelenkt werden: auch so lässt sich ein Verschlüsselungseffekt erreichen.




Besonders interessant könnte der Einsatz dieses Verfahrens auf Smartphones sein, denn dort ist die Auflösung des Displays besonders hoch und die Lage der Pixel ist relativ zum Rand bis auf den Zehntel-Millimeter genau bestimmt, so dass zwei Schienen - eine längs und eine quer - die Linsen-Karte genau justieren könnten.




Wichtig für den praktischen Einsatz ist die Wiederverwendbarkeit der Linsen-Karte. Deshalb ergibt sich die Fragestellung: Wie kann man unter bestimmten Annahmen erreichen, dass eine Karte möglichst oft benutzt werden kann, ohne dass ein Angreifer auf dem Smartphone, der ja die Bilder auf dem Display sieht und durch paarweises Vergleichen analysieren könnte, Schlüsse ziehen kann.

Betreuer: Dr. Bernd Borchert, Dr. Klaus Reinhardt
http://www-fs.informatik.uni-tuebingen.de/~borchert/Troja/