The Trusted Agent Model
Defeating Privacy Enhancement using Seals

Paulo Mateus\textsuperscript{1} and Serge Vaudenay\textsuperscript{2}

\textsuperscript{1} SQIG /IT - DM/IST TULisbon
1049-001 Lisboa, Portugal
http://sqig.math.ist.utl.pt

\textsuperscript{2} EPFL
CH-1015 Lausanne, Switzerland
http://lasecwww.epfl.ch

\textbf{Abstract.} Some security properties rely on the fact that the agents have random access to their memory and computation. Herein, we assume that the adversaries \textit{would deliberately} cast themselves in a restrictive computation model just to be able to perform attacks. In this way, we show how tamper-proof hardware can be used to perform several offline privacy attacks, namely to undeniable and ring signatures. We formalize the attacks in the so called \textit{universal trusted agent model}. This defines an oracle relative to which zero-knowledge is impossible as soon as one-way functions exist. We conclude by the surprising philosophical assertion saying that the concept of sealing a device is incompatible with the notion of privacy: the ability to put boundaries in computing devices prevent from providing full control on how private data spreads.