

# Universal Steganography

Maciej Liškiewicz, Rüdiger Reischuk, Ulrich Wölfel

Institut für Theoretische Informatik, Universität zu Lübeck, Germany

**Abstract.** In order to embed secret messages reliably and without being detectable into unsuspecting covertexts, a stegosystem has to draw samples from a covertext source/channel to estimate the distribution. For stegosystems that use a black-box sampler (there is no a priori knowledge of the covertext distribution), an exponential lower bound (with respect to the length of the secret message) has been shown for the query complexity of the sampling procedure. However, it is assumed that the attacker has complete knowledge of the covertext distribution.

We consider a more fair and realistic situation where the stegoencoder and the attacker have the same state of knowledge concerning the covertext distribution. Both have to learn the distribution by sampling. It is investigated how algorithmic learning techniques can be used to design secure, reliable and computationally efficient stegosystems. Positive results are obtained on the one hand for covertext channels with simple descriptions (concepts and hypothesis spaces) and on the other hand for pseudorandom channels.