DOUGLAS STINSON, University of Waterloo

Unconditionally secure chaffing and winnowing with short authentication tags

Rivest proposed the idea of a chaffing-and-winnowing scheme, in which confidentiality is achieved through the use of an authentication code. Thus it would still be possible to have confidential communications even if conventional encryption schemes were outlawed. Hanaoka *et al.* constructed unconditionally secure chaffing-and-winnowing schemes which achieve perfect secrecy in the sense of Shannon. Their schemes are constructed from unconditionally secure authentication codes.

In this talk, we construct unconditionally secure chaffing-and-winnowing schemes from unconditionally secure authentication codes in which the authentication tags are very short. This could be a desirable feature, because certain types of unconditionally secure authentication codes can provide perfect secrecy if the length of an authentication tag is at least as long as the length of the plain text. The use of such a code might be prohibited if encryption schemes are made illegal, so it is of interest to construct chaffing-and-winnowing schemes based on "short" authentication tags.

We use elementary combinatorial techniques for our construction.