Unconditional Authenticity and Privacy from an Arbitrarily Weak Secret and Completely Insecure Communication

Stefan Wolf
Département d'informatique et de recherches opérationnelles
Université de Montréal
C.P. 6128, Succ. Centre-ville
Montréal, Québec
CANADA H3C 3J7

Abstract

Unconditional cryptographic security cannot be generated simply from scratch, but must be based on some given primitive to start with such as, most typically, a secret key. Whether or not this well-known fact necessarily leads to the conclusion that this type of security is impractical depends on how weak such basic primitives can be and how realistic it is therefore to realize or find them in—classical or quantum—reality. A natural way of minimizing the required resources for information-theoretic security is to reduce the LENGTH of the key. In this talk, we focus on its LEVEL OF PRIVACY instead and find that even if the communication channel is completely insecure, a common string an arbitrarily large part of which is known to the adversary can be used for achieving fundamental cryptographic goals such as message authenticity and confidentiality.

This is joint work with Renato Renner.