Establishing secret common randomness between two or multiple devices in a network resides at the root of communication security. In its most frequent form of key establishment, the problem is traditionally decomposed into a randomness generation stage (randomness purity is subject to employing often costly true random number generators) and an information-exchange agreement stage, which relies either on public-key infrastructure or on symmetric encryption (key wrapping).

This dissertation has been divided into two main parts. In the first part, an algorithm called KERMAN is proposed to establish secret-common-randomness for ad-hoc networks, which works by harvesting randomness directly from the network routing metadata, thus achieving both pure randomness generation and (implicitly) secret-key agreement. This algorithm relies on the route discovery phase of an ad-hoc network employing the Dynamic Source Routing protocol, is lightweight, and requires relatively little communication overhead. The algorithm is evaluated for various network parameters, and different levels of complexity, in OPNET network simulator. The results show that, in just ten minutes, thousands of secret random bits can be generated network-wide, between different pairs in a network of fifty users.

The proposed algorithm described in this first part of this research study has inspired the study of the problem of generating a secret key based on a more practical model to be explored in the second part of this dissertation. Indeed, the secret key establishment from common randomness has been traditionally investigated under certain limiting assumptions, of which the most ubiquitous appears to be that the information available to all parties comes in the form of independent and identically distributed (i.i.d.) samples of some correlated random variables. Unfortunately, models employing the i.i.d assumption are often not accurate representations of real scenarios.

A more capable model would represent the available information as correlated hidden Markov models (HMMs), based on the same underlying Markov chain. Such a model accurately reflects the scenario where all parties have access to imperfect observations of the same source random process, exhibiting a certain time dependency. In the second part of the dissertation, a computationally-efficient asymptotic bounds for the secret key capacity of the correlated-HMM scenario has been derived. The main obstacle, not only for this model, but also for other non-i.i.d cases, is the computational complexity. This problem has been addressed by converting the initial bound to a product of Markov random matrices, and using recent results regarding its convergence to a Lyapunov exponent.