A note on Shannon theorem on secure codes

L. Accardi, Y. G. Lu, M. Regoli

Roma II University and Bari University, Itary

Abstract

Abstract: In the past years the importance of Shannon's work on encryption and coding has been emphasized by many papers even outside information theory, where it is universally recognized (see e.g. [3], [5]). In the paper [1] Shannon introduced the notion of perfect encryption code, studied the mathematical structure of these codes and formulated a necessary condition for a code to be perfect. In this note we find a necessary and sufficient condition under assumptions more general than Shannon's ones (section B). In section C we point out that Shannon's perfect secrecy condition only involves the set of messages and the set of cryptograms but there is no assumption linking the set of keys with either of them. We introduce such a condition, quite natural from the cryptographic point of view, and we prove that this condition uniquely fixes the cryptogram probability distribution of secure codes to be the uniform one.