OSAMA BATAINEH, Univ. of Saskatchewan

Imprecise Probabilities for Cryptanalysis of Ciphertexts

In cryptography, secrecy of ciphertext decryption is important and crucial for protection against cipher cyber-attacks. In ciphertext decryption, the appropriate probabilistic model must be selected to measure on occurrences of ciphertext characters. In this poster, imprecise probabilities are used to reflect the differences in prior beliefs amongst cryptanalysts, on probabilities of occurrences of alphabetic characters in ciphertexts. They can be used to give larger margin for predicting the correct keywords for successful decryption of difficult ciphertexts. For each character, there will be lower and upper bound probabilistic estimates based on using Bayesian methods with sets of prior distributions. It is important to see how prior changes, based on imprecise probability models, can impact changes in posterior distributions of ciphertexts, and their decryptions. Furthermore, imprecise probabilities can establish for new understanding of concepts of "perfect secrecy", "redundancy" and "unicity distance" in ciphertext decryption procedures.