Cryptology ePrint Archive: Report 2011/610

An optimal Key Enumeration Algorithm and its Application to Side-Channel Attacks

Nicolas Veyrat-Charvillon and Benoît Gérard and Mathieu Renauld and François-Xavier Standaert

Abstract: Methods for enumerating cryptographic keys based on partial information obtained on key bytes are important tools in cryptanalysis. This paper discusses two contributions related to the practical application and algorithmic improvement of such tools. On the one hand, we observe that modern computing platforms allow performing very large amounts of cryptanalytic operations, approximately reaching 2^50 to 2^60 block cipher encryptions. As a result, cryptographic key sizes for such ciphers typically range between 80 and 128 bits. By contrast, the evaluation of leaking devices is generally based on distinguishers with very limited computational cost, such as Kocher's Diff erential Power Analysis. We bridge the gap between these cryptanalytic contexts and show that giving side-channel adversaries some computing power has major consequences for the security of leaking devices. For this purpose, we rst propose a Bayesian extension of non-profi led side-channel attacks that allows us to rate key candidates in function of their respective probabilities. Next, we investigate the impact of key enumeration taking advantage of this Bayesian formulation, and quantify the resulting reduction in the data complexity of the attacks. On the other hand, we observe that statistical cryptanalyses usually try to reduce the number and size of lists corresponding to partial information on key bytes, in order to limit the time and memory complexity of the key enumeration. Quite surprisingly, few solutions exist that allow an effi cient merging of large lists of subkey candidates. We provide a new deterministic algorithm that signi ficantly reduces the number of keys to test in a divide-and-conquer attack, at the cost of limited (practically tractable) memory requirements. It allows us to optimally enumerate key candidates from any number of (possibly redundant) lists of any size, given that the subkey information is provided as probabilities. As an illustration, we nally exhibit side-channel cryptanalysis experiments where the correct key candidate is ranked up to position 23^2, in which our algorithm reduces the number of keys to test o ine by an average factor 2^5 and a factor larger than 2^10 in the worst observed cases, compared to previous solutions. We also suggest examples of statistical attacks in which the new deterministic algorithm would allow improved results.

Category / Keywords: implementation / side-channel analysis

Date: received 10 Nov 2011

Contact author: nicolas veyrat at uclouvain be