Optimization of Wave Rejection Sampling

nicolas.sendrier@inria.fr, équipe-projet SECRET, Inria de Paris

Wave is a recent digital signature algorithm based on codes. Its core primitive consists in finding a ternary word of large Hamming weight whose syndrome has a prescribed value. In a nutshell it consists in inverting the syndrome function on a specific point.

This primitive uses a secret information, namely the hidden structure of a generalized \((U | U + V)\) ternary code, to efficiently find a suitable word. There are multiple (in fact exponentially many) solutions to this syndrome inversion problem and the inverse must be carefully selected in order to avoid leakage of secret information. This process is referred to as rejection sampling. Its purpose is to ensure that the output distribution of the digital signatures is independent from the particular secret key being used. In the case of Wave we want to ensure that, for any secret key and for uniformly random messages, the signature distribution is uniform among ternary words of given length \(n\) and Hamming weight \(w\).

Several levers are available to reach this target distribution:

- In each of the two steps of the decoding process, a part of the randomness is drawn according to a discrete distribution which is controlled by the algorithm. The choice of those two internal distributions affect the signature distribution and can bring it close to the target (uniform) distribution.

- This comes in conjunction with rejection vectors which are used to filter the results of two intermediate computations, one for each of the two decoding steps. Each computation uses one of the quantities drawn internally. If the result of the computation is filtered out, it is computed again with a different randomness. A proper choice of the rejection rules ensures that the output follows exactly the target distribution.

For any choice for the internal distributions there exist rejection vectors to reach the target distribution. This existence is guaranteed by a theoretical analysis. Moreover this analysis provides an effective mean to compute those rejection vectors as well as an average rejection rate. A measure of quality of the global rejection sampling process is precisely this average rejection rate.

Current solutions have been obtained from families of parameterisable internal distributions (derived from Laplace distributions). Though this led to relatively small rejection rates (one or a few percents typically), this approach offers little flexibility. Minimizing the average rejection rate is an optimization problem whose parameters are the internal distributions. Those distributions are discrete and the corresponding system of equations is linear, but on the other hand it is under-determined and highly constrained. The purpose of the internship is to devise new models to efficiently solve the problem, hopefully improving over the current solutions.

References