

ABSTRACT

Key Encapsulation Platform and Key Exchange Protocol

5 According to a first aspect of the invention, there is provided a blender module configured to: receive a plurality of input messages, with at least one having uniform randomness; aggregate the received plurality of input messages to propagate the uniform randomness of the at least one input message with uniform randomness; and generate, in a randomness blender function mode: a plurality of output messages, each having uniform randomness, wherein total entropy of the plurality of output messages
10 is less than or equal to total entropy of all input messages; or when at least one of the plurality of input messages lacks uniform randomness, a plurality of output messages, each with uniform randomness and dependency amongst all output messages where the uniform randomness of the plurality of output messages has a total entropy less than or equal to the total entropy of all input messages; or generate, in
15 a randomness extractor mode: an output message with uniform randomness.

Figure 1