ABSTRACT

An example embodiment provides a calculating method using a zero-knowledge proof-friendly one-way function, performed by a computing device, the calculating method including: calculating a first intermediate bit stream by inputting an input bit stream of a one-way function to an augmented matrix, calculating a second intermediate bit stream by dividing the first intermediate bit stream into a predetermined number of bit streams and inputting each of the predetermined number of divided bit streams to a substitution-box (S-box), and outputting an output bit stream of the one-way function by inputting the second intermediate bit stream to a reduced matrix.

FIG. 1