

ABSTRACT

METHOD AND APPARATUS FOR PERFORMING MODULAR ARITHMETIC

An apparatus and method is disclosed for performing the modular operation $S=AB \bmod N$. The apparatus is arranged such that the constant $J0$ which is ordinarily required in order to complete the operation is not required to be explicitly computed,
5 thus simplifying and speeding up the operation.

Figure 4



G00002

102102



162162