162162

G00002

ABSTRACT

APPARATUS FOR MULTIPRECISION INTEGER ARITHMETIC

A system and method for performing multiplication and modular reduction of large integers. The system includes at least one large integer unit (21), each large integer unit having a multiplier (22), an adder (23), and a register (24). First and second multiplier inputs are applied to the multiplier, and first and second adder inputs are applied to the adder. One output of the multiplier is also applied to the adder. A plurality of large integer units may be connected into a large integer unit array (39) that includes a complementing gate (35) and a latching register (34). A second output of the multiplier is applied to the first adder input of a next large integer unit, with processing speed increasing as additional large integer units are added to the array.

(Figure 2)