UMass | Dartmouth

Information Technology

Title:	***Approximate SRT Division Method (UMD 08-12)***
Inventors:	***Makia Powell***
Applications:	Improved algorithms for carrying out the mathematical division function for use by microprocessor manufacturers as well as chip or hardware makers.
Benefits:	Use of the algorithm exponentially reduces the number of entries in the quotient tables used by microchips, resulting in significant advantages in terms of cost, speed and improved operation.
Technology Description:	A critical feature of most encryption systems is the ability to perform division on very large numbers. However, performing division functions digitally on most microprocessors is much more difficult and resource hungry than performing addition, subtraction and multiplication. Existing algorithms for digital division fall into two main categories: slow division and fast division. Slow division algorithms produce one digit of the final quotient per iteration. Fast division methods start with a close approximation to the final quotient and produce twice as many digits of the final quotient on each iteration. One popular slow division method is known as SRT division, named from the Sweeny, Robertson, and Tocher algorithm. The present invention is an improvement on the SRT method, referred to as "Partial SRT". It depends on the fact that if any two numbers are known out to their first N digits, then the first N-1 digits of their product or division will be known. The algorithm allows the calculation of a speculative approximation, rounded up only to a certain decimal place, which can be corrected later in an iterative process.
Patent Status:	US Patent No. 8,725,786.

For more information:

Catherine Ives, PhD
Intellectual Property Consultant
Office of Technology Commercialization & Ventures (OTCV) Foster Administration Building, #008
University of Massachusetts Dartmouth
285 Old Westport Road
North Dartmouth, MA 02747
Email: cives@umassd.edu

Return to Available Inventions Page