平成１４年度　情報工学専攻修士論文要旨

高木 研究室	氏　　名	KAIHARA, MARCELO EMILIO
論 文 題 目	A VLSI Algorithm for Modular Multiplication/Division (剰余系乗除算のための VLSI アルゴリズム)	

The advent of Internet and electronic commerce introduced the necessity of managing several security protocols in PCs, mobile devices, such as PDAs, and smart cards. Since processing of public-key cryptographs requires huge amount of computation, the demand of developing small dedicated hardware for accelerating the calculations is increasing.

In this work, we propose an algorithm for modular multiplication/division suitable for VLSI implementation. In the algorithm, multiplication and division are combined so that the hardware requirement is reduced by making large part of the hardware components be shared by both operations. The algorithm is based on Montgomery's method for modular multiplication and on the extended Binary GCD algorithm for modular division. It can perform either of these two operations with a reduced amount of hardware. Both calculations are carried out through iterations of simple operations such as shifts, additions and subtractions. The radix-2 signed-digit representation is employed so that all additions and subtractions are performed without carry propagation. Inputs and output are also expressed in the same redundant representation so that the output can be fed back into the inputs to allow chained multiplications in applications such as modular exponentiation. The original Montgomery's algorithm has been modified and accelerated so that it can process two digits at a time. The extended Binary GCD algorithm has also been further accelerated. As a result, we obtained a fast algorithm with almost all the hardware components shared for both operations.

A modular multiplier/divider based on this algorithm has a linear array structure with a bit-slice feature. It carries out an n-bit modular multiplication in at most $\lfloor \frac{2(n+2)}{3} \rfloor + 3$ clock cycles, and an n-bit modular division in at most $2n + 5$ clock cycles where the length of the clock cycle is constant and independent of n.

We have designed a modular multiplier/divider based on this algorithm and estimated the circuit area and delay. We found that an n-bit modular multiplier/divider can be implemented without increasing the circuit delay and with similar hardware amount to that of the multiplier and divider considered separately.

Publications

• Marcelo E. Kaihara and Naofumi Takagi, "A Modulo M Multiplier/Divider," Technical Report of IEICE., VLD2002-109, pp.163-168, Nov. 2002, Japan.
• Marcelo E. Kaihara and Naofumi Takagi, "A VLSI Algorithm for Modular Multiplication/Division," paper accepted for publication in Proc. 16th IEEE Symp. on Computer Arithmetic, to be held in June 2003, Spain.
• Marcelo E. Kaihara and Naofumi Takagi, "A Modular Multiplication/Division Algorithm for VLSI," paper to be published in CS sessions at the 2003 IEICE Gen. Conf. to be held in March 2003, Japan.