平成１５年度　情報工学専攻修士論文要旨

高木 研究室	氏　　名	郭　　晶
論 文 題 目	Hardware Algorithm for Multiplication/Division on GF(2^m) (GF(2^m) 上の乗算/除算のハードウェアアルゴリズム)	

With the proliferation of Internet usage, there is an increasing necessity for PCs and mobile devices, such as PDAs, of having ability to manage several security protocols. Since processing of public-key cryptosystems requires huge amount of computation, there is a growing demand for developing dedicated hardware to accelerate this. Arithmetic operations in GF(2^m) play important roles in such cryptosystems, where m is very large, i.e., several hundreds.

In this paper, we propose a hardware algorithm for multiplication /division in GF(2^m). We combine multiplication and division so that the hardware requirement is reduced by making large part of the circuit be shared by the two operations. In the hardware algorithm, multiplication is based on Montgomery's algorithm in GF(2^m) and division is based on the extended Binary GCD algorithm for GF(2^m). It can perform either of these two operation through iteration of simple operations, such as shifts, bitwise exclusive-OR and AND operations.

The multiplier/divider based on the algorithm has a linear array structure with a bit-slice feature and carries out division in $2m$ clock cycles and multiplication in m clock cycles. The amount of hardware is proportional to m and the depth is a constant independent of m .