**発表概要**

# モンゴメリ乗算法の高速化

テイ チョユウ[†] 太田昌孝[†]
松本尚[††] 荒木純道[†]

モンゴメリ乗算法は高速な剰余乗算法の 1 つである．一方，レジスタブロッキング手法やキャリーセーブ手法などは多倍長乗算に有効であることが知られている．本研究では，これらの手法を多倍長演算に対応するモンゴメリ乗算法に実装した．Intel 社の Itanium2（900 MHz）と Pentium4（2.2 GHz）上の C 言語実装で，従来型多倍長モンゴメリ乗算法と高速化された多倍長モンゴメリ乗算法の処理速度を比較した．Itanium2（900 MHz）上の 44,160 ビット剰余乗算に対して，高速型の処理速度は従来型より約 8.37 倍が得られた．Pentium4（2.2 GHz）上の 11,520 ビット剰余乗算に対して，高速型の処理速度は従来型より約 2.16 倍が得られた．

# High Performance Montgomery Multiplication

Zheng Chuyu,[†] Mastaka Ohta,[†] Takashi Matsumoto[††] and Kiyomichi Araki[†]

Montgomery multiplication is a fast modular multiplication method. It is known that register blocking and carry save techniques etc. are effectively applied in multiprecision multiplications. In this research, we implemented the multiprecision Montgomery multiplication with these techniques. We make comparison of processing speed between original multiprecision Montgomery multiplication and improved multiprecision Montgomery multiplication on Intel Pentium4 (2.2 GHz) processor and Intel Itanium2 (900 MHz). For the implementation of Itanium2 (900 MHz) processor, it is obtainable that the processing speed of 44,160 bits of modular multiplication would be increased to 8.37 times as fast as original one. For the implementation of Pentium4 (2.2 GHz) processor, it is obtainable that the processing speed of 11,520 bits of modular multiplication would be increased to 2.16 times as fast as original one.

（平成 17 年 1 月 21 日発表）

† 東京工業大学情報理工学研究科
Graduate School of Information Science and Engineering, Tokyo Institute of Technology
†† 国立情報学研究所情報基盤研究系
Foundations of Informatics Research Division, National Institute of Informatics