# CORR 2000-36

## On Modular Reduction

**Huapeng Wu**

**Abstract** In this paper, an algorithm to partially evaluate modular reduction without division is proposed. A proof of the correctness of the algorithm is given. For a family of generalized Mersenne numbers $N = 2^n - 2^m - 1,\ 0 < m < \frac{n+1}{2}$, we show that the modular reduction operation $A \bmod N$, where $A < N^2$, can be reduced to

$$A \bmod N \equiv A_1 + A_2 + A_4 + 2^m(A_3 + A_4),$$

where $A \triangleq A_1 + A_2 \times 2^n,\ 0 \le A_1 \le 2^n - 1$, and $A_2 \triangleq A_3 + A_4 \times 2^{n-m} - 1$. For another family of generalized Mersenne numbers $N = 2^n - 2^m - 2^{m_1} - 1,\ 0 < m_1 < m < \frac{n+1}{2}$, we find that the modular reduction operation $A$ and $N$, where $A < N^2$, can be partially solved as

$$\begin{aligned} A \bmod N \quad \equiv \quad & A_1 + A_2 + A_4 + A_6 + 2^m(A_3 + A_4 + A_6) + \\ & 2^{m_1}(A_3 + A_4 + A_6 + A_5 \times 2^{n-m}), \end{aligned}$$

where $A \triangleq A_1 + A_2 \times 2^n,\ 0 \le A_1 \le 2^n - 1,\ A_2 \triangleq A_3 + A_4 \times 2^{n-m},\ 0 \le A_3 \le 2^{n-m} - 1$, and $A_4 \triangleq A_5 + A_6 \times 2^{m-m-1} - 1$.

**Keywords** Modular arithmetic, public-key cryptosystems.