Published in *Electronics Letters* **33(23):1931, 1997.**

Normalisation in diminished-radix modulus transformation

J.-F. Dhem, M. Joye and J.-J. Quisquater

Indexing terms: Number theory, Digital arithmetic

Modular multiplication goes faster if the modulus has a diminished radix (DR) form. The authors quantify precisely the number of bits necessary to transform any modulus into its DR form.

Introduction: In numerous applications, modular multiplications have to be performed. For example, to encrypt a message M with the RSA cryptosystem [1], we compute the corresponding ciphertext $C = M^e \bmod N$. Assuming that the computations modulo $N' = \delta \cdot N$ are faster, then the computation of C can be speeded up by

$$C = \frac{\Big(\delta\,(M^e \bmod N')\Big) \bmod N'}{\delta} \ .$$

Such ideas were exploited by Quisquater [2, 3], and later by Walter [4].

Diminished-radix modulus transformation: Let $\sum_{i=0}^{n-1} \nu_i\, 2^i$ and $\sum_{i=0}^{n'-1} \nu'_i\, 2^i$ be the binary expansion of N and N', respectively. The modulus N' is called *DR modulus* [5] if it has the special form

$$N' = \delta\, N = 2^{n'} - \mu, \tag{1}$$

where $\delta, \mu < 2^n$, and $n' = n + c$.

A valid choice for the normalisation factor δ is $\lfloor 2^{n'}/N \rfloor$. However, the full division by N is not necessary to obtain the value of δ as we shall see in the following theorem.

Theorem ([6]): Let $k = n-c-2$, and let $\sum_{i=0}^{n-1} \nu_i\, 2^i$ be the binary expansion of N. Putting $\hat{N} = \sum_{i=k}^{n-1} \nu_i\, 2^{i-k}$, if we define

$$\hat{\delta} = \left\lfloor \frac{2^{2c+2}}{\hat{N}} \right\rfloor \tag{2}$$

then $\delta \leq \hat{\delta} \leq \delta + 1$.

Proof: (i) Immediately, we have

$$\delta = \left\lfloor \frac{2^{n'}}{\sum_{i=0}^{n-1} \nu_i\, 2^i} \right\rfloor \leq \left\lfloor \frac{2^{n'}}{2^k \sum_{i=k}^{n-1} \nu_i\, 2^{i-k}} \right\rfloor = \left\lfloor \frac{2^{2c+2}}{\hat{N}} \right\rfloor = \hat{\delta} \ .$$

(ii) Since $\nu_{n-1} = 1$, it follows that $\hat{N} \geq 2^{n-1-k} = 2^{c+1}$. Hence,

$$\hat{\delta} = \left\lfloor \frac{2^{2c+2}}{\hat{N}} \right\rfloor = \left\lfloor \frac{2^{2c+2}}{\hat{N}+1} \left(1 + \frac{1}{\hat{N}}\right) \right\rfloor \leq \left\lfloor \frac{2^{2c+2}}{\hat{N}+1} \right\rfloor + 1 \ .$$

Therefore, we obtain

$$\begin{aligned} \delta &= \left\lfloor \frac{2^{n'}}{\sum_{i=0}^{n-1} \nu_i\, 2^i} \right\rfloor = \left\lfloor \frac{2^{n+c}}{\hat{N}\, 2^k + \sum_{i=0}^{k-1} \nu_i\, 2^i} \right\rfloor \\ &\geq \left\lfloor \frac{2^{n+c-k}}{\hat{N}+1} \right\rfloor = \left\lfloor \frac{2^{2c+2}}{\hat{N}+1} \right\rfloor \geq \hat{\delta} - 1 \ . \end{aligned}$$

■

Conclusion: If we take $\hat{\delta}$ as an approximation for δ, the error is at most one. Therefore, with only one test, we obtain the exact value of the normalisation factor δ from only the $(c+2)$ highest bits of N.

Acknowledgements: We are grateful to D. Veithen for some fruitful comments.

5 September 1997

M. Joye (*UCL Crypto Group, Dép. de Mathématique (AGEL), Université catholique de Louvain, Chemin du Cyclotron 2, B-1348 Louvain-la-Neuve, Belgium*)

J.-F. Dhem and J.-J. Quisquater (*UCL Crypto Group, Dép. d'Électricité (DICE), Université catholique de Louvain, Place du Levant 3, B-1348 Louvain-la-Neuve, Belgium*)

E-mail: joye@agel.ucl.ac.be / {dhem, jjq}@dice.ucl.ac.be

References

1 RIVEST, R. L., SHAMIR, A., and ADLEMAN, L.: 'A method for obtaining digital signatures and public-key cryptosystems', *Commun. ACM*, 1978, **21**, pp. 120–126

2 QUISQUATER, J.-J.: 'Fast modular exponentiation without division', presented at the rump session of EUROCRYPT '90, Aarhus, Denmark, 1990

3 QUISQUATER, J.-J.: 'Procédé de codage selon la méthode dite RSA par un micro-contrôleur et dispositifs utilisant ce procédé'. Demande de brevet français, No. de dépôt 9002274, (U.S. Patent #5,166,978), 25 February 1990

4 WALTER, C. D.: 'Faster modular multiplication by operand scaling'. Proceedings of CRYPTO '91 (Springer-Verlag, 1992), pp. 313-323

5 ORTON, G., PEPPARD, L., and TAVARES, S.: 'A design of a fast pipelined modular multiplier based on a diminished-radix algorithm', *Journal of Cryptology*, 1993, **6**, pp. 183-208

6 JOYE, M.: 'Arithmétique algorithmique: Application au crypto-système à clé publique RSA'. Thesis for MS in Applied Mathematics, Jan. 1994, Université catholique de Louvain