
G. Hanrot a, P. Zimmermann b

a CNRS, ENS de Lyon, Inria, UCBL, Université de Lyon; Laboratoire LIP, 46 allée d’Italie, F-69364 Lyon cedex 07, France
b Centre de recherche Inria Nancy – Grand Est, Équipe-projet CARAMEL – bâtiment A, 615 rue du jardin botanique, F-54600 Villers-lès-Nancy, France

A R T I C L E  I N F O
Article history:
Received 17 February 2014
Accepted 17 February 2014
Available online 17 March 2014

Keywords:
Mulders’ algorithm
Karatsuba model

A B S T R A C T
We correct a minor mistake in the paper of Hanrot and Zimmermann (2004).

© 2014 Elsevier Ltd. All rights reserved.

In Algorithm ShortProduct (Hanrot and Zimmermann, 2004, pp. 394–395), at the final step, read

\[
\text{return } (\ell(x^2) + xm(x^2) + x^2 h(x^2)) \mod x^n.
\]

In the printed version, the result might have degree \(n\): if \(n\) is odd from the term \(xm(x^2)\), or if \(n\) is even from \(x^2 h(x^2)\).

The proof of Theorem 2 actually only proves that the result of Algorithm ShortProduct is congruent to \(fg\) modulo \(x^n\), not that it has degree \(< n\). With the correction above, this is obvious. Note that it does not change the number of ring operations as it is merely a truncation step.

DOI of original article: http://dx.doi.org/10.1016/j.jsc.2003.03.001.
E-mail addresses: guillaume.hanrot@ens-lyon.fr (G. Hanrot), paul.zimmermann@inria.fr (P. Zimmermann).
Acknowledgements

The authors would like to thank Bill Allombert and Karim Belabas for pointing this mistake.

References