Ferradi, Houda; **Géraud, Rémi**; **Maimuţ, Diana**; **Naccache, David**; **Zhou, Hang**
Backtracking-assisted multiplication. (English) Zbl 1384.68008
Cryptogr. Commun. 10, No. 1, 17-26 (2018).

Summary: This paper describes a new multiplication algorithm, particularly suited to lightweight microprocessors when one of the operands is known in advance. The method uses backtracking to find a multiplication-friendly encoding of the operand known in advance. A 68HC05 microprocessor implementation shows that the new algorithm indeed yields a twofold speed improvement over classical multiplication for 128-byte numbers.

MSC:

68M07 Mathematical problems of computer architecture
68W40 Analysis of algorithms
94A60 Cryptography

Keywords:

multiplication; integer arithmetics; backtracking

Full Text: DOI

References:

[1] Avižienis, A.: Signed-digit number representations for fast parallel arithmetic. IRE Trans. Electron. Comput. \textbf{EC-10}(3):389-400. https://doi.org/10.1109/TEC.1961.5219227 (1961)

[2] Barrett, P.: Implementing the Rivest Shamir and Adleman public key encryption algorithm on a standard digital signal processor. In: Odlyzko, A M (ed.) Advances in Cryptology—CRYPTO'86, volume 263 of Lecture Notes in Computer Science, Santa Barbara, CA, USA, August 1987, pp 311-323. Springer, Heidelberg (1987)

[3] Bernstein, R, Multiplication by integer constants, Softw. Pract. Exp., 16, 641-652, (1986)

[4] Cappello, PR; Steiglitz, K, Some complexity issues in digital signal processing, IEEE Trans. Acoust. Speech Signal Process., 32, 1037-1041, (1984) · Zbl 0578.68035

[5] Certivox. The MIRACL big number library. See https://www.certivox.com/miracl

[6] Cook, S.A.: On the minimum computation time of functions. PhD thesis (1966) · Zbl 0578.68035

[7] Dempster, AG; Macleod, MD, Constant integer multiplication using minimum adders, IEE Proc.—Circ. Dev. Syst., 141, 407-413, (1994) · Zbl 0814.68080

[8] Dempster, A.G., Macleod, M.D.: Use of Multiplier Blocks to Reduce Filter Complexity. In: 1994 IEEE International Symposium on Circuits and Systems, ISCAS, 1994, pp. 263-266. London, England (1994). https://doi.org/10.1109/ISCAS.1994.409247 · Zbl 0659.94006

[9] Diffie, W; Hellman, ME, New directions in cryptography, IEEE Trans. Inf. Theory, 22, 644-654, (1976) · Zbl 0435.94018

[10] ElGamal, T.: On computing logarithms over finite fields. In: Williams, H.C. (ed.) Advances in Cryptology—CRYPTO'85, volume 218 of Lecture Notes in Computer Science, Santa Barbara, CA, USA, August 18-22, 1986, pp 396-402. Springer, Heidelberg (1986) · Zbl 0223.68007

[11] Feige, U., Fiat, A., Shamir, A.: Zero knowledge proofs of identity. In: Aho, A. (ed.) 19th Annual ACM Symposium on Theory of Computing, pp. 210-217, New York City, NY, USA, May 25-27, 1987. ACM Press (1987) · Zbl 0659.94006

[12] Feige, U; Fiat, A; Shamir, A, Zero-knowledge proofs of identity, J. Cryptol., 1, 77-94, (1988) · Zbl 0659.94006

[13] Fürer, M, Faster integer multiplication, SIAM J. Comput., 39, 979-1005, (2009) · Zbl 1192.68926

[14] Harvey, D., Van Der Hoeven, J., Lecerf, G.: Even faster integer multiplication. arXiv preprint arXiv:1407.3360 (2014) · Zbl 1350.68145

[15] Karatsuba, A., Ofman, Y.: Multiplication of many-digital numbers by automatic computers. Doklady Akad. Nauk SSSR \textbf{145}, 293-294 (1962) · Zbl 0435.94018

[16] Knuth, D.: The Art of Computer Programming (1968) · Zbl 0191.17903

[17] Montgomery, PL, Modular multiplication without trial division, Math. Comput., 44, 519-521, (1985) · Zbl 0559.10006

[18] Schönhage, A; Strassen, V, Schnelle multiplikation grosser zahlen, Computing, 7, 281-292, (1971) · Zbl 0223.68007

[19] Toom, AL, The complexity of a scheme of functional elements realizing the multiplication of integers, Soviet Math. Dokl., 3,

714-716, (1963) · Zbl 0203.15604

[20] Wu, H; Hasan, MA, Closed-form expression for the average weight of signed-digit representations, IEEE Trans. Comput., 48, 848-851, (1999) · Zbl 1392.68062