Jiří Tůma, Jiří Vábek

On the number of binary signed digit representations of a given weight

Comment.Math.Univ.Carolin. 56,3 (2015) 287 –306.

Abstract: Binary signed digit representations (BSDR's) of integers have been studied since the 1950's. Their study was originally motivated by multiplication and division algorithms for integers and later by arithmetics on elliptic curves. Our paper is motivated by differential cryptanalysis of hash functions. We give an upper bound for the number of BSDR's of a given weight. Our result improves the upper bound on the number of BSDR's with minimal weight stated by Grabner and Heuberger in *On the number of optimal base* 2 *representations*, Des. Codes Cryptogr. **40** (2006), 25–39, and introduce a new recursive upper bound for the number of BSDR's of any given weight.

Keywords: binary signed digit representation; NAF; minimal weight
AMS Subject Classification: 11A63, 68R01

References

[1] Booth A.D., *A signed binary multiplication technique*, Quart. J. Mech. Appl. Math. **4** (1951), 236–240.
[2] Reitwiesner G., *Binary arithmetic*, in Advances in Computers, 1, Academic Press, New York, 1960, pp. 231–308.
[3] Morain F., Olivos J., *Speeding up the computations on an elliptic curve using addition-subtraction chains*, RAIRO Inform. Théor. Appl. **24** (1990), 531–543.
[4] Koyama K., Tsuruoka Y., *Speeding up elliptic cryptosystems by using a signed binary window method*, Advances in cryptology - CRYPTO' 92, Lecture Notes in Comput. Sci., 740, Springer, Berlin, 1993, pp. 345–357.
[5] Miyaji A., Ono T., Cohen H., *Efficient elliptic curve exponentiation*, Information and Communications Security, Lecture Notes in Comput. Sci., 1334, Springer, Berlin-Heidelberg, 1997, pp. 282–290.
[6] Solinas J., *Efficient arithmetic on Koblitz curves*, Des. Codes Cryptogr. **19** (2000), 195–249.
[7] Oswald E., Aigner M., *Randomized addition-subtraction chains as a countermeasure against power attacks*, Cryptographic Hardware and Embedded Systems – CHES 2001, Lecture Notes in Comput. Sci., 2162, Springer, Berlin, 2001, pp. 39–50.
[8] Ha J., Moon S., *Randomized signed-scalar multiplication of ECC to resist power attacks*, Cryptographic Hardware and Embedded Systems – CHES 2002, Lecture Notes in Comput. Sci., 2523, Springer, Berlin-Heidelberg, 2002, pp. 551–563.
[9] Ebeid N., Anwar Hasan M., *On randomized private keys to counteract DPA attacks*, in Matsui M., Zuccherato R. (ed.), SAC 2003, Lecture Notes in Comput. Sci., 3006, Springer, Berlin, 2004, pp. 58–72.
[10] Heuberger C., *Minimal expansions in redundant number systems: Fibonacci bases and greedy algorithm*, Period. Math. Hungar. **49** (2004), no. 2, 65–89.
[11] Xiaoyu R., Katti R., *Left-to-right optimal signed-binary representation of a pair of integers*, IEEE Trans. Comput. **54** (2005), 132–140.
[12] Muir J.A., Stinson D.R., *Minimality and other properties of the width-w nonadjacent form*, Math. Comp. **75** (2006), no. 253, 369–384.
[13] Heuberger C., Prodinger H., *Analysis of alternative digit sets for nonadjacent representations*, Monatsh. Math. **147** (2006), 219–248.
[14] Grabner P.J., Heuberger C., *On the number of optimal base* 2 *representations*, Des. Codes Cryptogr. **40** (2006), 25–39.
[15] Stevens M., Lenstra A., de Weger B., *Chosen-prefix collisions for MD*5 *and colliding X*.509 *certificates for different identities*, Advances in cryptology – EUROCRYPT 2007 (Moni Naor, ed.), Lecture Notes in Comput. Sci., 4515, Springer, Berlin, 2007, pp. 1–22.
[16] Kim T.H., Han D., Okeya K., Lim J.I., *Differential power analysis on countermeasures using binary signed digit representations*, ETRI Journal, vol. 29, no. 5, Oct. 2007, pp. 619–632.

[17] Bang-ju Wang, Huan-guo Zhang, Zhang-yi Wang, Yu-hua Wang, *Speeding up scalar multiplication using a new signed binary representation for integers*, Multimedia Content Analysis and Mining, Lecture Notes in Comput. Sci., 4577, Springer, Berlin-Heidelberg, 2007, pp. 277–285.

[18] Vábek J., Joščák D., Boháček M., Tůma J., *A new type of* 2*-block collisions in MD*5, in Chowdury, Rijmen, Das (ed.), Progress in cryptology – INDOCRYPT 2008, Lecture Notes in Comput. Sci., 5365, Springer, Berlin, 2008, pp. 78-90.

[19] Wu T., Zhang M., Du H., Wang R., *On optimal binary signed digit representation of integers*, Appl. Math. J. Chinese Univ. Ser.B **25** (2010), no. 3, 331–340.

[20] Avanzi R., Heuberger C., Prodinger H., *Redundant τ-adic expansions I: non-adjacent digit sets and their applications to scalar multiplication*, Des. Codes Cryptogr. **58** (2011), no. 2, 173–202.