Povzetek

V uvodu diplomskega dela predstavimo seštevalne verige, njihove izpeljanke in njihovo povezavo s problemom potenciranja. V drugem poglavju pregledamo različne osnovne metode za sestavljanje učinkovitih seštevalnih verig. Obravnavamo dvojiško in m-tiško metodo, ki sestavita splošno uporabne seštevalne verige, ter metodo, ki temelji na neenoličnih zapisih števila in je uporabna predvsem v primeru, ko je deljenje časovno enakovredno množenju. V tretjem poglavju posplošimo metode iz drugega poglavja na metode z uporabo vnaprej naračunanih oken ter obravnavamo možne izboljšave te metode. Četrto poglavje uporablja predračunanje, kjer nekaj dela opravimo vnaprej in lahko nato učinkoviteje potenciramo neko fiksno osnovo na različne eksponente. Najprej obravnavamo metodo BGMW, nato še njeno izpeljanko, metodo Lim-Lee. V naslednjem poglavju se ukvarjamo s končnimi polji. Prvi razdelek tega poglavja predstavi posebnosti končnih polj ter splošne učinkovite algoritme za potenciranje v končnem polju $GF(p^n)$. Dalje se ukvarjamo še z učinkovitim potenciranjem v polinomski bazi v $GF(2^n)$ in generacijo normalne baze za $GF(p^n)$. Na koncu predstavimo še učinkovito metodo za potenciranje na posebne eksponente, katerih m-tiški zapis je sestavljen iz samih enic. V zadnjem poglavju najprej predstavimo aritmetiko v grupi eliptične krivulje, nato pa si ogledamo še učinkovito metodo za potenciranje elementov v grupi eliptične krivulje za posebne primere eliptičnih krivulj, ki jih imenujemo Koblitzove eliptične krivulje.

Klasifikacija MSC (2000): 68W30, 68Q25, 11Y16
Klasifikacija CCS (2005): F.2.1, G.4

Ključne besede:
aritmetika, potenciranje, hitro računanje, algoritem, končni obseg, eliptična krivulja
Keywords:
arithmetics, exponentiation, fast computation, algorithm, finite field, elliptic curve

Literatura

[1] S. Arno, F. S. Wheeler, Signed digit representations of minimal Hamming weight, *IEEE Trans. Comput. 42* (1993), str. 1007–1010

[2] E. F. Brickell, D. M. Gordon, K. S. McCurley, D. B. Wilson, *Fast Exponentiation with Precomputation (Extended Abstract)*, „Advances in Cryptology - Eurocrypt '92", v Lecture Notes in Comput. Sci. 658 (1993), str. 200–207

[3] J. Bos, M. Coster, *Addition chain heuristics*, „Advances in Cryptology—Proceedings of Crypto '89", v Lecture Notes in Comput. Sci. 435 (1990), str. 400–407

[4] P. Erdős, Remarks on number theory III, On addition chains, *Acta Arith. 6* (1960), str. 77–81

[5] S. Gao, J. von zur Gathen, D. Panario, V. Shoup, Algorithms for Exponentiation in Finite Fields, *J. Symbolic Comp. 29* (2000), str. 879–889

[6] D. M. Gordon, A Survey of Fast Exponentiation Methods, *J. Algorithms 27* (1998) str. 129–146

[7] D. E. Knuth, *The Art of Computer Programming Vol. 2, Seminumerical Algorithms*, 3. izdaja, Addison-Wesley, Reading, MA, 2003

[8] K. Koyama, Y. Tsuruoka, *Speeding up elliptic cryptosystems by using a signed binary window method*, „Advances in Cryptology—Proceedings of Crypto '92", v Lecture Notes in Comput. Sci. 740 (1993), str. 345–357

[9] R. Lidl, H. Niederreiter, *Finite Fields*, 2. izdaja, Cambridge Univ. Press, 1997

[10] C. H. Lim, P. J. Lee, More Flexible Exponentiation with Precomputation, „Advances in Cryptology—Proceedings of Crypto '94", v Lecture Notes in Comput. Sci. 839 (1994), str. 95–107

[11] J. Olivos, On vectorial addition chains, *J. Algorithms 2* (1981), str. 13–21

[12] A. Schönhage, A lower bound for the length of addition chains, *Theoret. Comput. Sci. 1* (1975), str. 1–12,

[13] J. H. van Lint, *Introduction to Coding Theory*, Springer-Verlag, Berlin/New York, 1982

[14] J. von zur Gathen, Efficient and optimal exponentiation in finite fields, *Comput. Complexity 1* (1991), str. 360–394

[15] J. von zur Gathen, J. Gerhard, *Modern computer algebra*, Cambridge University Press, Cambridge, 1999

[16] J. von zur Gathen, M. Nöcker, Computing special powers in finite fields, *Math. Comp. 73* (2003), str. 1499–1523