Povzetek

V tem delu smo vpeljali Čebiševe baze za končne obsege. Le–te omogočajo precejšnje izboljšanje kvadriranja, korenjenja in invertiranja elementov končnih obsegov. Opisali smo konstrukcijo Čebiševih baz iz optimalnih normalnih baz ter nekatere osnovne lastnosti. Izpeljali smo tudi izboljšane in hitrejše algoritme, zato je najbolj pomemben element dela implementacija celotne aritmetike Čebiševih baz, kar nam omogoča natančno analizo osnovnih in izboljšanih algoritmov ter primerjavo med njimi. Spoznali smo tudi algebraične osnove končnih obsegov in eliptičnih krivulj. Nenazadnje smo definirali napade s stranskim kanalom na kriptosisteme z eliptičnimi krivuljami ter možne načine zaščite algoritmov.

Ključne besede: eliptične krivulje, končni obsegi, aritmetična teorija števil

Abstract

In this thesis we define Chebyshev basis for finite fields. They allow us better square, square root and inverse calculations in finite fields. We describe the construction of Chebyshev basis from the optimal normal basis and include some basic properties. We also develop faster and optimized algorithms. This makes the implementation of all algorithms in Chebyshev basis the most important part of this thesis. It allows the analysis and comparison of algorithms. We also describe some basics about finite fields and elliptic curves. At the end we define side channel attacks on elliptic curve cryptosystems and possible protection of algorithms against them.

Key words: elliptic curves, finite fields, computational number theory

Math. subj. class: 14H52, 11T71, 11Y16 2006

Literatura

[1] T. Itoh, S. Tsuji *A fast Algorithm for Computing Multiplicative Inverses in* $\mathbb{F}_{2^m}$ *Using Normal Bases*, Information and Computation, Volume 78, Issue 3: 171–177, 1988.

[2] A. Jurišić, *Umbral optimal normal bases*, rokopis.

[3] P. L. Montgomery, *Speeding the Pollard and elliptic curve methods of factorization*, Mathematics of computation, 48(177): 243–264, 1987.

[4] I. F. Blake, Gadiel Serioussi, Nigel P. Smart, *Advances in elliptic curve cryptography*, London mathematical society, Canbridge university press, 2005.

[5] D. Hankerson, A. Menezes, S. Vanstone, *Guide to elliptic curve cryptography*, Springer 2004.

[6] D. Hankerson, J. L. Hernandez and A. Menezes, *Software implementation of elliptic curve cryptography over binary fields*, Cryptographic hardware and embedded systems - CHES 2000, 2000.

[7] A. Menezes, I. F. Blake, X. Gao, R. C. Mullin, S. A. Vanstone, T. Yaghoobian, *Applications of finite fields*, The International Series in Engineering and Computer Science, Springer, 1993.

[8] J. S. Coron, *Resistance against differential power analysis for elliptic curve cryptosystems*, In C.K. Koc and C. Paar, editors, *Cryptographic Hardware and embedded systems CHES 99*, volume 1717 of lecture notes in computer science, pages 292–302, Springer-Verlag, 1999.

[9] D. H. Stinson, *Some observations on parallel algorithms for fast exponentiation in* $GF(2^n)$, SIAM J. Computing 19: 711-717, 1990.

[10] J. Von Zur Gathen, *Efficient and optimal exponentiation in finite fields*, Computational Complexity 1: 360-394, 1991.

[11] V. Nastran, *Baze binarnih končnih obsegov*, Diplomsko delo, Fakulteta za matematiko in fiziko, Univerza v Ljubljani, Ljubljana, 2003.