POVZETEK

V tem diplomskem delu je poudarek na bilinearni preslikavi, imenovani Weilovo parjenje, ki se uporablja v številnih shemah za šifriranje z eliptičnimi krivuljami in tudi za reševanje problema diskretnega algoritma na eliptičnih krivuljah. Za izpeljavo definicije Weilovega parjenja je potrebno poznati osnove teorije deliteljev, zato so v diplomsko delo vključene tudi te. Predstavljen je tudi konkreten primer sheme, kjer je uporabljeno takšno parjenje. Poimenovana je shema za šifriranje s certifikati, saj v njej certifikat uporabljamo tudi kot odšifrirni ključ.

Na začetku je predstavljen osnovni model sheme za šifriranje s certifikati in po definiciji Weilovega parjenja so podrobneje opisani še algoritmi, v katerih se parjenje uporablja. Na koncu je podan opis razširjene sheme, kjer se z uporabo pokritja množice uporabnikov z veljavnim certifikatom zmanjša računska zahtevnost na strani certifikatne agencije.

Ključne besede: kriptografija, sheme za šifriranje, IBE, CBE, preklic certifikata, Weilovo parjenje, teorija deliteljev

ABSTRACT

The main topic of this thesis is a billinear map called Weil pairing. It is used in many elliptic curve cryptosystems. The definiton of Weil pairing cannot be given without some knowledge of the divisor theory. I also present an example of an encryption scheme, in which Weil pairing is used. It is called certificate-based encryption by its author Craig Gentry. In this scheme a certificate acts also as a decryption key.

First, the basic model of certificate-based encryption is presented. After the definiton of the Weil pairing the algorithms with Weil pairing are described in detail. Finally, the incremental scheme is described, in which computation costs of the certificate authority are dramatically improved with the use of subset covers.

Keywords: cryptography, encryption shemes, IBE, CBE, certificate revocation, Weil pairing, divisor theory

Math. Subj. Class. (2000): 94A60, 11T71, 14G50, 14H52

Literatura

[1] C. Gentry, *Certificate-Based Encription and the Certificate Revocation Problem*, Advances in Cryptology - EUROCRYPT 2003, LNCS 2656, str. 272–293, Springer, 2003.

[2] S. Micali, *Efficient Certificate Revocation*, Technical Report TM-542b, MIT Laboratory for Computer Science, 1996.
(dostopno na http://portal.acm.org/citation.cfm?id=889659)

[3] A. Enge, *Elliptic Curves and Their Applications to Cryptography - An Introduction*, Kluwer Academic Publishers, 1999.

[4] I. Vidav, *Eliptične krivulje in eliptične funkcije*, Drutvo matematikov, fizikov in astronomov Slovenije, 1991.

[5] J. Barbič, *Schoofov algoritem*, Diplomsko delo, Univerza v Ljubljani, Fakulteta za matematiko in fiziko, 2000.

[6] A. Shamir, *Identity-Based Cryptosystems and Signature Schemes*, Advances in Cryptology, Proceedings of CRYPTO '84, LNCS 196, str. 47–53, Springer, 1984.

[7] D. Boneh in M. Franklin, *Identity-Based Encryption from the Weil pairing*, Advances in Cryptology - CRYPTO 2001, LNCS 2139, str. 213–229, Springer, 2001.

[8] E. Fujisaki in T. Okamoto, *Secure integration of asymmetric and symmetric encryption*, Advances in Cryptology - CRYPTO '99, LNCS 1666, str. 537–554, Springer, 1999.

[9] D. Boneh, B. Lynn in H. Shacham, *Short Signatures from the Weil Pairing*, Advances in Cryptology - ASIACRYPT 2001, LNCS 2248, str. 514–532, Springer, 2001.

[10] D. Boneh, C. Gentry, B. Lynn in H. Shacham, *Aggregate and Verifiably Encrypted Signatures from Bilinear Maps*, Advances in Cryptology - EUROCRYPT 2003, LNCS 2656, str. 416–432, Springer, 2003.

[11] D. Naor, M. Naor in J. Lotspicch, *Revocation and Tracing Schemes for Stateless Receivers*, Advances in Cryptology - CRYPTO 2001, LNCS 2139, str. 41–62, Springer, 2001.

[12] P.S.L.M. Barreto, H.Y. Kim, B. Lynn in M. Scott, *Efficient Algorithms for Pairing-Based Cryptosystems*, Advances in Cryptology - CRYPTO 2002, LNCS 2442, str. 354–368, Springer, 2002.

[13] W. Aiello, S. Lodha in R. Ostrovsky, *Fast Digidal Identity Revocation*, Advances in Cryptology - CRYPTO '98, LNCS 1462, str. 137–152, Springer, 1998.

[14] D. Boneh, X. Ding, G. Tsudik in M. Wong, *A Method for Fast Revocation of Public Key Certificates and Security Capabilities*, Proc. of 10th Annual USENIX Security Symposium, 2001.
(dostopno na http://crypto.stanford.edu/˜dabo/pubs.html)

[15] R. Canetti, S. Halovi in J. Katz, *A Forward-Secure Public-Key Encryption Scheme*, Advances in Cryptology - EUROCRYPT 2003, LNCS 2656, str. 255–271, Springer, 2003.

[16] A. Menezes, T. Okamoto in S. Vanstone, *Reducing elliptic curve logarithms to logarithms in a fnite field*, IEEE Tran. on Info. Th., Vol. 39, str. 1639–1646, 1993.

[17] A. Joux in K. Nguyen, *Separating Decision Diffe-Hellman from Diffe-Hellman in cryptographic groups*, Journal of Cryptology 16, str. 239–247, 2003.

[18] A. J. Menezes, *Elliptic Curve Public Key Cryptosystems*, Kluwer Academic Publishers, 1993.

[19] L.S Charlap in D. P. Robbins, *An Elementary Introduction to Elliptic Curves*, CRD Expository Report No. 31, 1988.
(dostopno na: http://www.idaccr.org/reports/reports.html)

[20] L.S Charlap in R. Coley, *An Elementary Introduction to Elliptic Curves II*, CRD Expository Report 34, 1990.
(dostopno na: http://www.idaccr.org/reports/reports.html)

[21] M. Maas, *Pairing-Based Cryptography*, Master's Thesis, Technische Universiteit Eindhoven, 2004.
(dostopno na: http://paginas.terra.com.br/informatica/paulobarreto/pblounge.html)

[22] J.H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1986.

[23] J. D. van den Heiden, *Weil Pairing and the Drinfeld Modular Curve*, Rijksuniversiteit Groningen, 2003.
(dostopno na: http://dissertations.ub.rug.nl/faculties/science/2003/g.j.van.der.heiden/)

[24] S. Micali, *Novomodo: Scalable Certificate Validation and Simplified PKI Management*, Proc. of 1st Annual PKI Research Workshop, 2002.
(dostopno na: http://www.cs.dartmouth.edu/ pki02/Micali/)