## Podpisni shemi DSA in ECDSA po standardih FIPS 186-4 DSS in ANS X9.62-2005


### Povzetek

V tem diplomskem delu obravnavamo podpisno shemo DSA, kakršna je definirana v standardu FIPS 186-4 DSS, ter podpisno shemo ECDSA, kakršna je definirana v standardih FIPS 186-4 DSS in ANS X9.62-2005.

Na začetku razložimo matematično ozadje, ki je potrebno za razumevanje teh dveh podpisnih shem. Posebej pokažemo splošno razvejitveno lemo, kakršno sta predstavila Bellare in Neven. Na kratko predstavimo še kriptografske zgoščevalne funkcije. V četrtem poglavju nato na splošno predstavimo digitalne podpise in podpisne sheme. Podpisne sheme tudi formalno definiramo, jih razvrstimo ter opišemo vrste napadov na njih.

V petem in šestem poglavju podrobneje predstavimo podpisni shemi DSA in ECDSA. Vsako podpisno shemo definiramo, predstavimo nekatere najpomembnejše algoritme za ustvarjanje domenskih parametrov, javnega in zasebnega ključa, skrivnega števila ter za podpisovanje in preverjanje podpisov. Navedemo rezultate, povezane z dokazljivo varnostjo, dokažemo pravilnost in opišemo nekatere znane napade. Pri podpisni shemi DSA z uporabo splošne razvejitvene leme pokažemo še varnost pred napadom s ključem v Brickellovem modelu.


## Signature schemes DSA and ECDSA according to the standards FIPS 186-4 DSS in ANS X9.62-2005


### Abstract

In the current thesis, we deal with the signature scheme DSA, as defined in the standard FIPS 186-4 DSS, as well as the signature scheme ECDSA, as defined in the standards FIPS 186-4 DSS in ANS X9.62-2005.

In the beginning, we explain the mathematical background necessary to understand the two signature schemes. In particular, we prove general forking lemma as presented by Bellare and Neven. We then provide a brief outline of cryptographic hash functions. In the fourth chapter, we provide a general presentation of digital signatures and signature schemes formally defining signature schemes, classifying them and providing a description of attack types against such.

In the fifth and the sixth chapter, we present signature schemes DSA and ECDSA in detail. Each signature scheme is defined. We present some of the most important algorithms for generating domain parameters, public/private keys, secret numbers, and for signing/verifying signatures. We present the results relating to provable security, prove the correctness and describe some of the known attacks. In addition, we use general forking lemma and the Brickell model to prove the security of the signature scheme DSA against key-only attack.



**Math. Subj. Class. (2010):** 94A60, 11T71, 14G50, 68P25

**Ključne besede:** digitalni podpisi, kriptografija, eliptične krivulje, razvejitvena lema, dokazljiva varnost, DSA, ECDSA

**Keywords:** digital signatures, cryptography, elliptic curves, forking lemma, provable security, DSA, ECDSA

# Literatura


[1] *ANS X9.62 2005 Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)*. standard. 2005.

[2] S. Arora in B. Barak. *Computational complexity, A modern approach*. Cambridge University Press. Cambridge. 2009.

[3] D. W. Ash. I. F. Blake in S. A. Vanstone. *Low complexity normal bases*. Discrete Applied Mathematics **25** (1989). 191–210.

[4] E. Bach. *Discrete logarithms and factoring*. 1984. URL: `http://digitalassets.lib.berkeley.edu/techreports/ucb/text/CSD-84-186.pdf` (pridobljeno 7. 6. 2016).

[5] C. Bader in sod.. *On the Impossibility of Tight Cryptographic Reductions*. Cryptology ePrint Archive. Report 2015/374. 2015. URL: `http://eprint.iacr.org/2015/374` (pridobljeno 25. 6. 2016).

[6] J. Barbič. *Schoofov algoritem*. diplomska naloga, Univerza v Ljubljani. 2000.

[7] E. Barker. *SP 800-57 Recommendation for Key Management Part 1: General*. National Institute of Standards in Technology (NIST), jan. 2016. URL: `http://dx.doi.org/10.6028/nist.sp.800-57pt1r4` (pridobljeno 7. 6. 2016).

[8] E. Barker. *SP 800-89 Recommendation for Obtaining Assurances for Digital Signature Applications*. National Institute of Standards in Technology (NIST). nov. 2006. URL: `http://csrc.nist.gov/publications/nistpubs/800-89/SP-800-89_November2006.pdf` (pridobljeno 26. 6. 2016).

[9] E. B. Barker in A. L. Roginsky. *SP 800-131A Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*. National Institute of Standards in Technology (NIST), nov. 2015. URL: `http://dx.doi.org/10.6028/nist.sp.800-131ar1` (pridobljeno 7. 6. 2016).

[10] M. Bellare in G. Neven. *Multi-signatures in the Plain public-Key Model and a General Forking Lemma*. v: Proceedings of the 13th ACM Conference on Computer and Communications Security CCS '06, ACM. New York. 2006. 390–399.

[11] M. Bellare in P. Rogaway, *Random Oracles Are Practical: A Paradigm for Designing Efficient Protocols*, v: Proceedings of the 1st ACM Conference on Computer and Communications Security CCS '93, ACM, New York, 1993, 62–73.

[12] I. F. Blake, G. Seroussi in N. P. Smart, *Elliptic curves in cryptography*, London Mathematical Society Lecture Note Series **265**, Cambridge University Press, Cambridge, 2000.

[13] I. F. Blake, G. Seroussi in N. P. Smart, ur., *Advances in elliptic curve cryptography*, London Mathematical Society Lecture Note Series **317**, Cambridge University Press, Cambridge, 2005.

[14] E. Brickell in sod., *Design Validations for Discrete Logarithm Based Signature Schemes*, v: Public Key Cryptography: Third International Workshop on Practice and Theory in Public Key Cryptosystems, PKC 2000, Melbourne, Victoria, Australia, January 18-20, 2000. Proceedings (H. Imai in Y. Zheng), Springer, Berlin Heidelberg, 2000, 276–292.

[15] E. Brickell in sod., *Design Validations for Discrete Logarithm Based Signature Schemes*, v: Public Key Cryptography: Third International Workshop on Practice and Theory in Public Key Cryptosystems, PKC 2000, Melbourne, Victoria, Australia, January 18-20, 2000. Proceedings (H. Imai in Y. Zheng), Berlin, Heidelberg: Springer Berlin Heidelberg, 2000, 276–292.

[16] D. R. Brown, *The Exact Security of ECDSA*, teh. poročilo, URL: `http://cacr.uwaterloo.ca/techreports/2000/corr2000-54.ps` (pridobljeno 9. 7. 2016).

[17] B. B. Brumley in N. Tuveri, *Remote Timing Attacks Are Still Practical*, v: Proceedings of the 16th European Conference on Research in Computer Security ESORICS'11, Springer-Verlag, Berlin, Heidelberg, 2011, 355–371.

[18] R. Canetti, O. Goldreich in S. Halevi, *The Random Oracle Methodology, Revisited*, J. ACM **51** (4) (2004), 557–594.

[19] *Certicom ECC Challenge*, 2009, URL: `https://www.certicom.com/images/pdfs/challenge-2009.pdf` (pridobljeno 7. 6. 2016).

[20] H. Cohen in sod., ur., *Handbook of elliptic and hyperelliptic curve cryptography*, Discrete Mathematics and its Applications (Boca Raton), Chapman & Hall/CRC, Boca Raton, FL, 2006.

[21] I. Connell, *Elliptic Curve Handbook*, 1996, URL: `https://pendientedemigracion.ucm.es/BUCM/mat/doc8354.pdf` (pridobljeno 25. 6. 2016).

[22] T. H. Cormen in sod., *Introduction to algorithms, Third Edition*, MIT Press, Cambridge, MA, 2009.

[23] Q. H. Dang, *SP 800-107 Recommendation for applications using approved hash algorithms*, National Institute of Standards in Technology (NIST), 2012, URL: http://dx.doi.org/10.6028/nist.sp.800-107r1 (pridobljeno 7. 6. 2016).

[24] C. Diem, *On the discrete logarithm problem in elliptic curves*, Compos. Math. **147** (1) (2011), 75–104.

[25] J. K. Elaine Barker, *SP 800-90A Recommendation for Random Number Generation Using Deterministic Random Bit Generators*, National Institute of Standards in Technology (NIST), nov. 2006, URL: http://dx.doi.org/10.6028/NIST.SP.800-90Ar1 (pridobljeno 27. 6. 2016).

[26] T. Elgamal, *A public key cryptosystem and a signature scheme based on discrete logarithms*, IEEE Transactions on Information Theory **31** (1985), 469–472.

[27] *FIPS PUB 180-4 Secure Hash Standard (SHS)*, standard, National Institute of Standards in Technology (NIST), jul. 2015, URL: http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf (pridobljeno 7. 6. 2016).

[28] *FIPS PUB 186-2 Digital Signature Standard (DSS)*, standard, National Institute of Standards in Technology (NIST), jan. 2000, URL: http://csrc.nist.gov/publications/fips/archive/fips186-2/fips186-2.pdf (pridobljeno 7. 6. 2016).

[29] *FIPS PUB 186-4 Digital Signature Standard (DSS)*, standard, National Institute of Standards in Technology (NIST), jul. 2013, URL: http://dx.doi.org/10.6028/nist.fips.186-4 (pridobljeno 7. 6. 2016).

[30] *FIPS PUB 202 SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions*, standard, National Institute of Standards in Technology (NIST), jul. 2015, URL: http://dx.doi.org/10.6028/nist.fips.202 (pridobljeno 6. 7. 2016).

[31] G. Frey in H.-G. Rück, *A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves*, Mathematics of computation **62** (1994), 865–874.

[32] O. Goldreich, *Foundations of cryptography, Basic tools*, Cambridge University Press, Cambridge, 2001.

[33] S. Goldwasser, S. Micali in R. L. Rivest, *A digital signature scheme secure against adaptive chosen-message attacks*, SIAM Journal on Computing **17** (1988), 281–308.

[34] *Standardisation in the field of Electronic Identities and Trust Service Providers Inventory of activities Version 1.0, December 2014*, European Union Agency for Network in Information Security (ENISA), dec. 2014, URL: https://

www.enisa.europa.eu/publications/standards-eidas/at_download/fullReport (pridobljeno 7. 6. 2016).

[35] D. Hankerson, A. Menezes in S. Vanstone, *Guide to elliptic curve cryptography*, Springer Professional Computing, Springer-Verlag, New York, 2004.

[36] J. E. Hopcroft, R. Motwani in J. D. Ullman, *Introduction to automata theory, languages, and computation*, Pearson Education Limited, Essex, 2006.

[37] D. Johnson, A. Menezes in S. Vanstone, *The Elliptic Curve Digital Signature Algorithm (ECDSA)*, International Journal of Information Security **1** (2001), 36–63.

[38] J. Katz in Y. Lindell, *Introduction to modern cryptography*, CRC Press, Boca Raton, 2007.

[39] J. Kelsey in B. Schneier, *Second Preimages on n-Bit Hash Functions for Much Less than $2^n$ Work*, v: Advances in Cryptology – EUROCRYPT 2005: 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22-26, 2005. Proceedings (R. Cramer), Springer, Berlin Heidelberg, 2005, 474–490.

[40] N. Koblitz in A. J. Menezes, *Another look at "provable security"*, J. of Cryptology **20** (2007), 3–37.

[41] P. C. Kocher, *Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems*, v: Advances in Cryptology — CRYPTO '96: 16th Annual International Cryptology Conference Santa Barbara, California, USA August 18–22, 1996 Proceedings (N. Koblitz), Springer, Berlin Heidelberg, 1996, 104–113.

[42] Y. Lindell, *How To Simulate It - A Tutorial on the Simulation Proof Technique*, Cryptology ePrint Archive, Report 2016/046, 2016, URL: http://eprint.iacr.org/2016/046 (pridobljeno 18. 7. 2016).

[43] M. Medwed in E. Oswald, *Template Attacks on ECDSA*, v: Information Security Applications: 9th International Workshop, WISA 2008, Jeju Island, Korea, September 23-25, 2008, Revised Selected Papers (K.-I. Chung, K. Sohn in M. Yung), Springer, Berlin Heidelberg, 2009, 14–27.

[44] A. J. Menezes, T. Okamoto in S. A. Vanstone, *Reducing elliptic curve logarithms to logarithms in a finite field*, IEEE Transactions on Information Theory **39** (1993), 1639–1646.

[45] A. J. Menezes, P. C. van Oorschot in S. A. Vanstone, *Handbook of applied cryptography*, CRC Press Series on Discrete Mathematics and its Applications, CRC Press, Boca Raton, 1996.

[46] R. C. Mullin in sod., *Optimal normal bases in $GF(p^n)$*, Discrete Applied Mathematics **22** (1989), 149–161.

[47] P. Nose, *Varnostna analiza protokolov za overjen dogovor o ključu in shem za digitalni podpis*, doktorska disertacija, Univerza v Ljubljani, 2014.

[48] D. Pointcheval in J. Stern, *Security Arguments for Digital Signatures and Blind Signatures*, J. Cryptology **13** (3) (2000), 361–396.

[49] D. Pointcheval in S. Vaudenay, *On provable security for digital signature algorithms*, 1996, URL: `http://infoscience.epfl.ch/record/99499/files/liens-96-17.ps` (pridobljeno 7. 6. 2016).

[50] T. Pornin, *Deterministic Usage of the Digital Signature Algorithm (DSA) and Elliptic Curve Digital Signature Algorithm (ECDSA)*, avg. 2013, URL: `http://dx.doi.org/10.17487/rfc6979` (pridobljeno 7. 6. 2016).

[51] T. Satoh in K. Araki, *Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves*, Commentarii Mathematici Universitatis Sancti Pauli **47** (1998), 81–92.

[52] I. Semaev, *Evaluation of discrete logarithms in a group of p-torsion points of an elliptic curve in characteristic p*, Mathematics of Computation of the American Mathematical Society **67** (1998), 353–356.

[53] V. Shoup, *Lower Bounds for Discrete Logarithms and Related Problems*, v: Advances in Cryptology — EUROCRYPT '97: International Conference on the Theory and Application of Cryptographic Techniques Konstanz, Germany, May 11–15, 1997 Proceedings (W. Fumy), Springer, Berlin Heidelberg, 1997, 256–266.

[54] N. P. Smart, *Cryptography, An introduction: Third edition*, URL: `https://www.cs.bris.ac.uk/~nigel/Crypto_Book/`.

[55] N. P. Smart in sod., *Algorithms, key size and parameters report – 2014*, European Union Agency for Network in Information Security (ENISA), nov. 2014, URL: `https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014/at_download/fullReport` (pridobljeno 7. 6. 2016).

[56] P. N. Smart, *The Discrete Logarithm Problem on Elliptic Curves of Trace One*, J. Cryptology **12** (3) (1999), 193–196.

[57] D. R. Stinson, *Cryptography: Theory and Practice, Third Edition*, Discrete Mathematics and its Applications (Boca Raton), Chapman & Hall/CRC, Boca Raton, 2006.

[58] S. Vaudenay, *Hidden Collisions on DSS*, v: Advances in Cryptology — CRYPTO '96: 16th Annual International Cryptology Conference Santa Barbara, California, USA August 18–22, 1996 Proceedings (N. Koblitz), Springer, Berlin Heidelberg, 1996, 83–88.

[59] S. Vaudenay, *The Security of DSA and ECDSA*, v: Public Key Cryptography — PKC 2003: 6th International Workshop on Practice and Theory in Public Key Cryptography Miami, FL, USA, January 6–8, 2003 Proceedings (Y. G. Desmedt), Springer, Berlin Heidelberg, 2002, 309–323.

[60] X. Wang, Y. L. Yin in H. Yu, *Finding Collisions in the Full SHA-1*, v: Advances in Cryptology – CRYPTO 2005: 25th Annual International Cryptology Conference, Santa Barbara, California, USA, August 14-18, 2005. Proceedings (V. Shoup), Springer, Berlin Heidelberg, 2005, 17–36.