Kriptovaluták elméleti háttere (VITMDV04)

Hivatkozások / References

Ladóczki Bence – BME VIK TMIT

References

[1] R. L. Rivest, A. Shamir, L. Adleman, *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, Communications of the ACM, 21(2):120–126, 1978.

[2] D. Coppersmith, *Finding a Small Root of a Univariate Modular Equation*, Advances in Cryptology – EUROCRYPT '96, Lecture Notes in Computer Science, vol. 1070, Springer, pp. 155–165, 1996.

[3] W. Diffie, M. E. Hellman, *New Directions in Cryptography*, IEEE Transactions on Information Theory, 22(6):644–654, 1976.

[4] National Bureau of Standards, *Data Encryption Standard (DES)*, FIPS PUB 46, 1977.

[5] J. Daemen, V. Rijmen, *The Design of Rijndael: AES – The Advanced Encryption Standard*, Springer, 2001.

[6] E. Rescorla, *The Transport Layer Security (TLS) Protocol Version 1.3*, RFC 8446, 2018.

[7] S. Vanstone, *Responses to NIST's Proposal*, Communications of the ACM, 35(7):50–52, 1992. (Válaszlevél, amelyben Vanstone az elliptikus görbék alkalmazását javasolja a DSA-hoz.)

[8] American National Standards Institute (ANSI), *X9.62: Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)*, 1998.

[9] L. M. Adleman, C. Pomerance, R. S. Rumely, *On Distinguishing Prime Numbers from Composite Numbers*, Annals of Mathematics, 117(1):173–206, 1983.

[10] S. Goldwasser, J. Kilian, *Almost All Primes Can Be Quickly Certified*, Proc. 18th Annual ACM Symposium on Theory of Computing, pp. 316–329, 1986.

[11] L. M. Adleman, M.-D. Huang, *Primality Testing and Abelian Varieties Over Finite Fields*, Lecture Notes in Mathematics, vol. 1512, Springer, 1992.

[12] M. Agrawal, N. Kayal, N. Saxena, *PRIMES is in P*, Annals of Mathematics, 160(2):781–793, 2004.

[13] P. W. Shor, *Algorithms for Quantum Computation: Discrete Logarithms and Factoring*, Proc. 35th Annual Symposium on Foundations of Computer Science, pp. 124–134, 1994.

[14] A. O. L. Atkin, F. Morain, *Elliptic Curves and Primality Proving*, Mathematics of Computation, 61(203):29–68, 1993.

[15] M. O. Rabin, *Probabilistic Algorithm for Testing Primality*, Journal of Number Theory, 12(1):128–138, 1980.

[16] J. P. Buhler, H. W. Lenstra Jr., C. Pomerance, *Factoring Integers with the Number Field Sieve*, in: A. K. Lenstra, H. W. Lenstra Jr. (eds.), The Development of the Number Field Sieve, Lecture Notes in Mathematics, vol. 1554, Springer, pp. 50–94, 1993.

[17] C. P. Schnorr, *Efficient Signature Generation by Smart Cards*, Journal of Cryptology, 4(3):161–174, 1991. (Első bemutatás: CRYPTO '89, Lecture Notes in Computer Science, vol. 435, pp. 239–252, Springer, 1990.)

[18] A. Fiat, A. Shamir, *How to Prove Yourself: Practical Solutions to Identification and Signature Problems*, Advances in Cryptology – CRYPTO '86, Lecture Notes in Computer Science, vol. 263, Springer, pp. 186–194, 1987.

[19] M. Bellare, P. Rogaway, *Random Oracles are Practical: A Paradigm for Designing Efficient Protocols*, Proceedings of the 1st ACM Conference on Computer and Communications Security, pp. 62–73, 1993.

[20] D. Pointcheval, J. Stern, *Security Proofs for Signature Schemes*, Advances in Cryptology – EUROCRYPT '96, Lecture Notes in Computer Science, vol. 1070, Springer, pp. 387–398, 1996.

[21] National Institute of Standards and Technology, *Digital Signature Standard (DSS)*, FIPS PUB 186, 1994.

[22] P. Wuille, J. Nick, T. Ruffing, *BIP 340: Schnorr Signatures for secp256k1*, Bitcoin Improvement Proposal, 2020.

[23] L. M. Adleman, *A Subexponential Algorithm for the Discrete Logarithm Problem with Applications to Cryptography*, Proc. 20th Annual IEEE Symposium on Foundations of Computer Science, pp. 55–60, 1979.

[24] N. Koblitz, *Hyperelliptic Cryptosystems*, Journal of Cryptology, 1(3):139–150, 1989.

[25] J. H. Silverman, *The Arithmetic of Elliptic Curves*, 2nd edition, Graduate Texts in Mathematics, vol. 106, Springer, 2009.

[26] L. C. Washington, *Elliptic Curves: Number Theory and Cryptography*, 2nd edition, Chapman & Hall/CRC, 2008.

[27] Certicom Research, *SEC 2: Recommended Elliptic Curve Domain Parameters*, Standards for Efficient Cryptography Group, Version 2.0, 2010.

[28] R. P. Gallant, R. J. Lambert, S. A. Vanstone, *Faster Point Multiplication on Elliptic Curves with Efficient Endomorphisms*, Advances in Cryptology – CRYPTO 2001, Lecture Notes in Computer Science, vol. 2139, Springer, pp. 190–200, 2001.

[29] D. Boneh, B. Lynn, H. Shacham, *Short Signatures from the Weil Pairing*, Advances in Cryptology – ASIACRYPT 2001, Lecture Notes in Computer Science, vol. 2248, Springer, pp. 514–532, 2001.

[30] Ethereum Foundation, *Ethereum 2.0 Specifications – Phase 0: The Beacon Chain*, 2020. https://github.com/ethereum/consensus-specs

[31] S. Bowe, *BLS12-381: New zk-SNARK Elliptic Curve Construction*, Zcash Engineering Blog, 2017. A görbe a Barreto–Lynn–Scott konstrukción alapul: P. S. L. M. Barreto, B. Lynn, M. Scott, *Constructing Elliptic Curves with Prescribed Embedding Degrees*, Security in Communication Networks – SCN 2002, Lecture Notes in Computer Science, vol. 2576, Springer, pp. 263–273, 2003. A BLS12-381 paramétereinek formális specifikációja: Ethereum Foundation, *BLS12-381 Curve Specification*, EIP-2537, 2020.

[32] Y. Lindell, *Simple Three-Round Multiparty Schnorr Signing with Full Simulatability*, Cryptology ePrint Archive, Report 2022/374, 2022.

[33] Y. Lindell, *Fast Secure Two-Party ECDSA Signing*, Advances in Cryptology – CRYPTO 2017, Lecture Notes in Computer Science, vol. 10402, Springer, pp. 613–634, 2017.

[34] A. Faz-Hernandez, S. Scott, N. Sullivan, R. S. Wahby, C. A. Wood, *Hashing to Elliptic Curves*, Internet Research Task Force (IRTF), RFC 9380, 2023.

[35] R. S. Wahby, D. Boneh, *Fast and Simple Constant-Time Hashing to the BLS12-381 Elliptic Curve*, Cryptology ePrint Archive, Report 2019/403, 2019.

[36] J. von Neumann, *Probabilistic Logics and the Synthesis of Reliable Organisms from Unreliable Components*, in: C. E. Shannon, J. McCarthy (eds.), Automata Studies, Annals of Mathematics Studies, No. 34, Princeton University Press, pp. 43–98, 1956.

[37] L. Lamport, *Time, Clocks, and the Ordering of Events in a Distributed System*, Communications of the ACM, 21(7):558–565, 1978.

[38] L. Lamport, *The Implementation of Reliable Distributed Multiprocess Systems*, Computer Networks, 2(2):95–114, 1978.

[39] L. Lamport, R. Shostak, M. Pease, *The Byzantine Generals Problem*, ACM Transactions on Programming Languages and Systems, 4(3):382–401, 1982.

[40] S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008. https://bitcoin.org/bitcoin.pdf

[41] V. Buterin, *Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform*, 2014. https://ethereum.org/en/whitepaper/

[42] Y. Sompolinsky, A. Zohar, *Secure High-Rate Transaction Processing in Bitcoin*, Financial Cryptography and Data Security, Lecture Notes in Computer Science, vol. 8975, Springer, pp. 507–527, 2015.

[43] S. Ellis, A. Juels, S. Nazarov, *ChainLink: A Decentralized Oracle Network*, 2017. https://chain.link/whitepaper

[44] V. Buterin, E. Conner, R. Dudley, M. Slipper, I. Norden, A. Bakhta, *EIP-1559: Fee Market Change for ETH 1.0 Chain*, Ethereum Improvement Proposals, 2019. https://eips.ethereum.org/EIPS/eip-1559

[45] I. Eyal, E. G. Sirer, *Majority is not Enough: Bitcoin Mining is Vulnerable*, Financial Cryptography and Data Security, Lecture Notes in Computer Science, vol. 8437, Springer, pp. 436–454, 2014.

[46] M. Mirkin, Y. Ji, J. Pang, A. Klages-Mundt, I. Eyal, A. Juels, *BDoS: Blockchain Denial-of-Service*, Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security (CCS), pp. 601–619, 2020.

[47] R. K. Konoth, E. Vineti, V. Moonsamy, M. Lindorfer, C. Kruegel, H. Bos, G. Vigna, *How You Get Shot in the Back: A Systematical Study about Cryptojacking in the Real World*, Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (CCS), pp. 1701–1713, 2018.

[48] J. Nash, *Equilibrium Points in N-Person Games*, Proceedings of the National Academy of Sciences, 36(1):48–49, 1950.

[49] N. van Saberhagen, *CryptoNote v 2.0*, 2013. https://www.getmonero.org/resources/research-lab/

[50] N. van Saberhagen, *CryptoNote v 2.0*, 2013. https://cryptonote.org/whitepaper.pdf

[51] S. Noether, *Ring Confidential Transactions*, Ledger, vol. 1, pp. 1–18, 2016.

[52] B. Bünz, J. Bootle, D. Boneh, A. Poelstra, P. Wuille, G. Maxwell, *Bulletproofs: Short Proofs for Confidential Transactions and More*, IEEE Symposium on Security and Privacy, pp. 315–334, 2018.

[53] T. Howard et al., *RandomX: ASIC-resistant Proof-of-Work Algorithm*, 2019. https://github.com/tevador/RandomX

[54] R. L. Rivest, A. Shamir, Y. Tauman, *How to Leak a Secret: Theory and Applications of Ring Signatures*, Lecture Notes in Computer Science, vol. 3895, Springer, pp. 164–186, 2006.

[55] B. Goodall, A. Noether, *Concise Linkable Ring Signatures and Forgery Against Adversarial Keys*, Monero Research Lab, 2019. https://eprint.iacr.org/2019/654

[56] Internal Revenue Service, *Pilot IRS Will Pay Up to $625,000 for Cryptocurrency Tracing Tools*, IRS Criminal Investigation, Request for Information RFI-CI-20-0006, 2020.

[57] European Parliament and Council, *Regulation (EU) 2023/1114 on Markets in Crypto-Assets (MiCA)*, Official Journal of the European Union, L 150/52, 2023.

[58] European Banking Authority, *Guidelines on the Transfer of Funds and Certain Crypto-Assets Regulations*, EBA/GL/2024/09, 2024.

[59] European Parliament and Council, *Regulation (EU) 2023/1113 on Information Accompanying Transfers of Funds and Certain Crypto-Assets (Recast)*, Official Journal of the European Union, L 150/1, 2023.

[60] A. Shamir, *How to Share a Secret*, Communications of the ACM, 22(11):612–613, 1979.

[61] R. Canetti, N. Makriyannis, U. Peled, *Fast Secure Multiparty ECDSA with Practical Distributed Key Generation and Applications to Cryptocurrency Custody*, Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security (CCS), pp. 1837–1851, 2022.

[62] Fireblocks, *MPC-CMP: Threshold ECDSA from Cryptographic Multiparty Computation*, Fireblocks Whitepaper, 2020. https://www.fireblocks.com/what-is-mpc/

[63] Curv (acquired by PayPal, 2021), *Institutional Digital Asset Infrastructure*. https://www.curv.co

[64] P. MacKenzie, M. K. Reiter, *Two-Party Generation of DSA Signatures*, Advances in Cryptology – CRYPTO 2001, Lecture Notes in Computer Science, vol. 2139, Springer, pp. 137–154, 2001.

[65] V. S. Miller, *The Weil Pairing, and Its Efficient Calculation*, Journal of Cryptology, 17(4):235–261, 2004.

[66] A. Weil, *Variétés abéliennes et courbes algébriques*, Hermann, Paris, 1948.

[67] A. J. Menezes, T. Okamoto, S. A. Vanstone, *Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field*, IEEE Transactions on Information Theory, 39(5):1639–1646, 1993.

[68] A. Joux, *A One Round Protocol for Tripartite Diffie–Hellman*, Algorithmic Number Theory Symposium (ANTS-IV), Lecture Notes in Computer Science, vol. 1838, Springer, pp. 385–393, 2000.

[69] D. Boneh, M. Franklin, *Identity-Based Encryption from the Weil Pairing*, Advances in Cryptology – CRYPTO 2001, Lecture Notes in Computer Science, vol. 2139, Springer, pp. 213–229, 2001.

[70] G. Frey, H.-G. Rück, *A Remark Concerning m-Divisibility and the Discrete Logarithm in the Divisor Class Group of Curves*, Mathematics of Computation, 62(206):865–874, 1994.

[71] R. Göbel, P. Keeler, A. E. Krzesinski, P. G. Taylor, *Bitcoin Blockchain Dynamics: The Selfish-Mine Strategy in the Presence of Propagation Delay*, Performance Evaluation, vol. 104, pp. 23–41, 2016.

[72] A. Back, *Hashcash – A Denial of Service Counter-Measure*, 2002. http://www.hashcash.org/papers/hashcash.pdf

[73] Block.one, *EOS.IO Technical White Paper v2*, 2018. https://github.com/EOSIO/Documentation

[74] J. Sun, *TRON: Advanced Decentralized Blockchain Platform*, 2018. https://tron.network/static/doc/white_paper_v_2_0.pdf

[75] Counterparty Foundation, *Counterparty: Protocol Specification*, 2014. https://counterparty.io

[76] C. Yocom-Piatt, *Decred: An Autonomous Digital Currency*, 2016. https://docs.decred.org/

[77] D. Mazières, *The Stellar Consensus Protocol: A Federated Model for Internet-level Consensus*, Stellar Development Foundation, 2015.

[78] M. Castro, B. Liskov, *Practical Byzantine Fault Tolerance*, Proceedings of the Third Symposium on Operating Systems Design and Implementation (OSDI), pp. 173–186, 1999.

[79] J. Kwon, *Tendermint: Consensus without Mining*, 2014. https://tendermint.com/static/docs/tendermint.pdf

[80] M. J. Fischer, N. A. Lynch, M. S. Paterson, *Impossibility of Distributed Consensus with One Faulty Process*, Journal of the ACM, 32(2):374–382, 1985.

[81] M. E. Hellman, *A Cryptanalytic Time-Memory Trade-Off*, IEEE Transactions on Information Theory, 26(4):401–406, 1980.

[82] H. Abusalah, J. Alwen, B. Cohen, D. Khilko, K. Pietrzak, L. Reyzin, *Beyond Hellman's Time-Memory Trade-Offs with Applications to Proofs of Space*, Advances in Cryptology – ASIACRYPT 2017, Lecture Notes in Computer Science, vol. 10625, Springer, pp. 357–379, 2017.

[83] D. Boneh, J. Bonneau, B. Bünz, B. Fisch, *Verifiable Delay Functions*, Advances in Cryptology – CRYPTO 2018, Lecture Notes in Computer Science, vol. 10991, Springer, pp. 757–788, 2018.

[84] Filecoin Team, *Proof of Replication and Proof of Spacetime*, Protocol Labs Technical Report, 2017. https://filecoin.io/proof-of-replication.pdf

[85] B. Cohen, K. Pietrzak, *The Chia Network Blockchain*, Chia Network, 2019. https://www.chia.net/assets/Chia-New-Consensus-0.9.pdf

[86] A. Haleem, A. Allen, A. Thompson, M. Nijdam, R. Tuesta, *Helium: A Decentralized Wireless Network*, Helium Systems Inc., 2019. http://whitepaper.helium.com

[87] D. Chaum, *Blind Signatures for Untraceable Payments*, Advances in Cryptology – CRYPTO '82, Springer, pp. 199–203, 1983.

[88] C. Dwork, M. Naor, *Pricing via Processing or Combatting Junk Mail*, Advances in Cryptology – CRYPTO '92, Lecture Notes in Computer Science, vol. 740, Springer, pp. 139–147, 1993.

[89] H. Ong, C. P. Schnorr, A. Shamir, *An Efficient Signature Scheme Based on Quadratic Equations*, Proceedings of the 16th Annual ACM Symposium on Theory of Computing, pp. 208–216, 1984.

[90] J. M. Pollard, *The Lattice Sieve*, Lecture Notes in Mathematics, vol. 1256, Springer, pp. 43–49, 1987.

[91] D. J. Bernstein, J. Buchmann, E. Dahmen (szerk.), *Post-Quantum Cryptography*, Springer, 2009. ISBN 978-3-540-88701-0.

[92] L. K. Grover, *A Fast Quantum Mechanical Algorithm for Database Search*, Proceedings of the 28th Annual ACM Symposium on Theory of Computing (STOC), pp. 212–219, 1996.

[93] R. Babbush, A. Zalcman, C. Gidney, M. Broughton, T. Khattar, H. Neven, T. Bergamaschi, J. Drake, D. Boneh, *Securing Elliptic Curve Cryptocurrencies against Quantum Vulnerabilities: Resource Estimates and Mitigations*, arXiv:2603.28846v2, 2026.

[94] J. Proos, Ch. Zalka, *Shor's Discrete Logarithm Quantum Algorithm for Elliptic Curves*, Quantum Information & Computation, 3(4):317–344, 2003. arXiv:quant-ph/0301141.

[95] M. Roetteler, M. Naehrig, K. M. Svore, K. Lauter, *Quantum Resource Estimates for Computing Elliptic Curve Discrete Logarithms*, Advances in Cryptology – ASIACRYPT 2017, LNCS 10625, pp. 241–270, Springer, 2017.

[96] T. Häner, S. Jaques, M. Naehrig, M. Roetteler, M. Soeken, *Improved Quantum Circuits for Elliptic Curve Discrete Logarithms*, Post-Quantum Cryptography (PQCrypto 2020), LNCS 12100, pp. 425–444, Springer, 2020.

[97] É. Gouzien, D. Ruiz, F.-M. Le Régent, J. Guillaud, N. Sangouard, *Performance Analysis of a Repetition Cat Code Architecture: Computing 256-bit Elliptic Curve Logarithm in 9 Hours with 126 133 Cat Qubits*, Physical Review Letters, 131:040602, 2023.

[98] D. Litinski, *How to Compute a 256-bit Elliptic Curve Private Key with Only 50 Million Toffoli Gates*, arXiv:2306.08585, 2023.

[99] C. Chevignard, P.-A. Fouque, A. Schrottenloher, *Reducing the Number of Qubits in Quantum Discrete Logarithms on Elliptic Curves*, Advances in Cryptology – EUROCRYPT 2026, Springer, 2026.

[100] H. Kim, K. Jang, S. Wang, V. Srivastava, A. Baksi, G. Song, H. Seo, A. Chattopadhyay, *New Quantum Circuits for ECDLP: Breaking Prime Elliptic Curve Cryptography*, IACR ePrint 2026/106, 2026.

[101] T. Toffoli, *Reversible Computing*, MIT Laboratory for Computer Science, Tech Memo MIT/LCS/TM-151, 1980.

[102] S. Bravyi, A. Kitaev, *Universal Quantum Computation with Ideal Clifford Gates and Noisy Ancillas*, Physical Review A, 71:022316, 2005.

[103] F. Arute et al., *Quantum Supremacy Using a Programmable Superconducting Processor*, Nature, 574:505–510, 2019.

[104] IBM Quantum, *IBM Unveils 1,121-Qubit Quantum Chip 'Condor'*, IBM Research Blog, 2023.

[105] Y. Zhu et al., *Quantum Computational Advantage via 60-Qubit 24-Cycle Random Circuit Sampling*, Science Bulletin, 67(3):240–245, 2022.

[106] NIST, *Module-Lattice-Based Key-Encapsulation Mechanism Standard (ML-KEM)*, FIPS 203, 2024.

[107] NIST, *Module-Lattice-Based Digital Signature Standard (ML-DSA)*, FIPS 204, 2024.

[108] NIST, *Stateless Hash-Based Digital Signature Standard (SLH-DSA)*, FIPS 205, 2024.

[109] R. J. McEliece, *A Public-Key Cryptosystem Based on Algebraic Coding Theory*, DSN Progress Report 42-44, Jet Propulsion Laboratory, pp. 114–116, 1978.

[110] D. Coppersmith, *An Approximate Fourier Transform Useful in Quantum Factoring*, IBM Research Report RC 19642, 1994. arXiv:quant-ph/0201067.

[111] M. A. Nielsen, I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, 2000.

[112] J. Koch, T. M. Yu, J. Gambetta, A. A. Houck, D. I. Schuster, J. Majer, A. Blais, M. H. Devoret, S. M. Girvin, R. J. Schoelkopf, *Charge-insensitive qubit design derived from the Cooper pair box*, Physical Review A, 76(4):042319, 2007.

[113] C. J. Ballance, T. P. Harty, N. M. Linke, M. A. Sepiol, D. M. Lucas, *High-Fidelity Quantum Logic Gates Using Trapped-Ion Hyperfine Qubits*, Physical Review Letters, 117(6):060504, 2016.

[114] E. Knill, R. Laflamme, G. J. Milburn, *A scheme for efficient quantum computation with linear optics*, Nature, 409(6816):46–52, 2001.

[115] D. Bluvstein, S. J. Evered, A. A. Geim, S. H. Li, H. Zhou, T. Manovitz, S. Ebadi, M. Cain, M. Kalinowski, D. Hangleiter, J. P. Bonilla Ataides, N. Maskara, I. Cong, X. Gao, P. Sales Rodriguez, T. Karolyshyn, G. Semeghini, M. J. Gullans, M. Greiner, V. Vuletić, M. D. Lukin, *Logical quantum processor based on reconfigurable atom arrays*, Nature, 626(7997):58–65, 2024.

[116] R. B. Griffiths, C.-S. Niu, *Semiclassical Fourier Transform for Quantum Computation*, Physical Review Letters, 76(17):3228–3231, 1996.

[117] D. Shanks, *Class Number, a Theory of Factorization, and Genera*, Proceedings of Symposia in Pure Mathematics, 20:415–440, AMS, 1971.

[118] J. M. Pollard, *Monte Carlo Methods for Index Computation (mod p)*, Mathematics of Computation, 32(143):918–924, 1978.

[119] V. Lyubashevsky, *Lattice Signatures Without Trapdoors*, Advances in Cryptology – EUROCRYPT 2012, LNCS 7237, pp. 738–755, Springer, 2012.