Bibliography

[1] KTH Royal Institute of Technology. *Canvas*. 2021. URL: https://www.kth.se/en/student/kth-it-support/learning-platforms/canvas/canvas-1.784659 (visited on 02/26/2021).

[2] Paul E. Black and Vreda Pieterse. *"data structure", in Dictionary of Algorithms and Data Structures [online]*. 2004. URL: http://www.nist.gov/dads/HTML/datastructur.html (visited on 02/26/2021).

[3] Peter Wegner and Edwin D. Reilly. "Data Structures". In: *Encyclopedia of Computer Science*. GBR: John Wiley and Sons Ltd., 2003, pp. 507–512. ISBN: 0470864125.

[4] Britannica, The Editors of Encyclopaedia. *"Data structure." Encyclopedia Britannica*. 2017. URL: https://www.britannica.com/technology/data-structure (visited on 02/26/2021).

[5] Henry M Walker. *Abstract data types: specifications, implementations, and applications*. Jones & Bartlett Learning, 1996.

[6] Ross J. Anderson. *Security Engineering: A Guide to Building Dependable Distributed Systems*. 2nd ed. Wiley Publishing, 2008. Chap. 2. ISBN: 9780470068526.

[7] Dieter Gollmann. *Computer Security*. USA: John Wiley & Sons, Inc., 1999. ISBN: 0471978442.

[8] Synopsys. *The Heartbleed Bug*. 2020. URL: https://heartbleed.com/ (visited on 05/05/2021).

[9] Jonathan Afek and Adi Sharabani. *Dangling Pointer*. 2007. URL: https://www.exploit-db.com/docs/english/17260-dangling-pointer.pdf (visited on 05/04/2021).

[10] Eyal Nussbaum and Michael Segal. “Skiplist Timing Attack Vulnerability”. In: *Data Privacy Management, Cryptocurrencies and Blockchain Technology*. Springer, 2019, pp. 49–58.

[11] Thomas H. Cormen et al. *Introduction to Algorithms, Third Edition*. 3rd. The MIT Press, 2009. ISBN: 0262033844.

[12] Hanjun Dai et al. *Adversarial Attack on Graph Structured Data*. 2018. arXiv: 1806.02371 [cs.LG].

[13] Scott A. Crosby and Dan S. Wallach. “Denial of Service via Algorithmic Complexity Attacks”. In: *12th USENIX Security Symposium (USENIX Security 03)*. Washington, D.C.: USENIX Association, Aug. 2003. URL: https://www.usenix.org/conference/12th-usenix-security-symposium/denial-service-algorithmic-complexity-attacks.

[14] T. Gerbet, A. Kumar, and C. Lauradoux. “The Power of Evil Choices in Bloom Filters”. In: *2015 45th Annual IEEE/IFIP International Conference on Dependable Systems and Networks*. 2015, pp. 101–112. DOI: 10.1109/DSN.2015.21.

[15] Kenny Paterson. *Probabilistic Data Structures in Adversarial Settings*. Keynote talk given by Kenny Paterson from ETH Zurich at CANS 2020. Dec. 2020. URL: https://www.youtube.com/watch?v=ASBFQgQcmWU (visited on 05/05/2021).

[16] Pedro Reviriego and Daniel Ting. *Security of HyperLogLog (HLL) Cardinality Estimation: Vulnerabilities and Protection*. 2020. arXiv: 2002.06463 [cs.CR].

[17] David Clayton, Christopher Patton, and Thomas Shrimpton. “Probabilistic Data Structures in Adversarial Environments”. In: *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*. CCS ’19. London, United Kingdom: Association for Computing Machinery, 2019, pp. 1317–1334. ISBN: 9781450367479. DOI: 10.1145/3319535.3354235. URL: https://doi.org/10.1145/3319535.3354235.

[18] Pedro Reviriego and David Larrabeiti. “Denial of Service Attack on Cuckoo Filter Based Networking Systems”. In: *IEEE Communications Letters* 24.7 (2020), pp. 1428–1432. DOI: 10.1109/LCOMM.2020.2983405.

[19] KTH Royal Institute of Technology. *Degree Programme in Computer Science and Engineering: Programme syllabuses*. 2021. URL: https://www.kth.se/student/kurser/program/CDATE?l=en (visited on 01/22/2021).

Appendix A

Mandatory Courses of CDATE

Table A.1 lists the mandatory courses of CDATE by the year they are scheduled to be taught. DD1390 and DD2300 spans over three and two years, respectively. Courses marked with (*) are courses which are fully dedicated to individual projects. Such courses were deemed non-applicable since students may study a variety of different topics for their projects.