



UNIVERSIDADE FEDERAL DO PARANÁ
DEPARTAMENTO DE INFORMÁTICA

Av. Cel. Francisco Heráclito dos Santos, 100 - Centro Politécnico, - -
Bairro Jardim das Américas, Curitiba/PR, CEP 81531-980

Telefone: 3360-5000 - <http://www.ufpr.br/>

Despacho nº 3208647/2020/UFPR/R/ET/DINF

Processo nº 23075.068556/2020-87

Subárea: Arquitetura de Computadores

Tópicos:

- 1 - Projeto de sistemas digitais, circuitos combinacionais, circuitos sequenciais, estratégias de sincronização e distribuição de relógio.
- 2 - Técnicas de projeto de sistemas digitais para minimizar dispêndio de energia e potência.
- 3 - Conjunto de instruções, "application binary interface", geração de código, otimização de código no "backend" do compilador.
- 4 - Projeto de processadores segmentados (pipeline) e super-escalares; interface com o sistema operacional, interrupções, exceções.
- 5 - Hierarquia de memória; memória virtual, segmentação, paginação, e sistemas de armazenagem (discos magnéticos, SSDs, NVRAM).
- 6- Circuitos aritméticos, somadores rápidos, multiplicadores combinacionais. Segmentação (pipelining) de circuitos aritméticos.

Bibliografia:

- FLOYD, Thomas L. Digital Fundamentals, Pearson, 2014, 11a ed.
- HARRIS, David; Harris, Sarah. Digital Design and Computer Architecture, O'Reilly, 2012, 2a ed.
- HENNESSY, John L; PATTERSON, David A. Computer Architecture: A Quantitative Approach, Morgan Kaufmann, 2012, 5a ed.
- JACOB, Bruce L; W~Ng, Spencer; Wang, David T. Memory Systems: Cache, DRAM, Disk, Morgan Kaufmann, 2008.
- KATZ, Randy H; BORRIELLO, Gaetano. Contemporary Logic Design, Prentice Hall, 2004.
- MANO, M Morris; KIME, Charles R. Logic and Computer Design Fundamentals, Prentice Hall, 2000, 2a ed.
- PATTERSON, David A; HENNESSY, John L. Computer Organization & Design: The Hardware/Software Interface, Morgan Kaufmann, 2014, 5a ed.
- SHEN, John Paul; LIPASTI, Mikko H, Modern Processor Design: Fundamentals of Superscalar Processors, McGraw-Hill, 2005.
- SWEETMAN, Dominic. See MIPS Run -- Linux, Morgan Kaufmann, 2007, 2a ed.
- TAUB, Herbert. Digital Circuits and Microprocessors, McGraw-Hill, 1982.

Subárea: Informática na Educação

Tópicos:

- 1 - Educação à Distância, Ensino Remoto e Ensino online
- 2 - Educação em Computação
- 3 - Objetos de Aprendizagem
- 4 - Pensamento Computacional e Ensino de Programação
- 5 - Robótica Educacional
- 6 - Sistemas Tutoriais Inteligentes

Bibliografia:

- BELLONI, Maria L. Educação a distância. 6. ed. Campinas, SP: Autores Associados, 2012.
- CALVÃO, Leandro Dantas; PIMENTEL, Mariano; FUKS, Hugo. Do email ao Facebook: Uma perspectiva evolucionista sobre os meios de conversação da internet. Rio de Janeiro: UNIRIO, 2014.
- DEWEY, John (1916). Democracy and Education: An Introduction to the Philosophy of Education. New York: Macmillan.
- NKAMBOU, Roger; MIZOGUCHI, Riichiro; BOURDEAU, Jacqueline (Ed.). Advances in intelligent tutoring systems. Springer Science & Business Media, 2010.
- PIMENTEL, Mariano; SANTOS, Edméa; SAMPAIO, Fábio Ferrentini. Informática na educação. CEIE-SBC: 2020. Online: <https://ieducacao.ceie-br.org/>
- SANTOS, Edméa. Pesquisa-formação na cibercultura. Teresina: EDUFPI, 2019.
- PAPERT, Seymour A. Mindstorms: Children, computers, and powerful ideas. Basic books, 2020.
- BARBOSA, Rodrigo, and Paulo Blikstein. Robótica Educacional: Experiências Inovadoras na Educação Brasileira. Penso Editora. 2019.
- DENNING, Peter J., and Matti Tedre. Computational thinking. MIT Press, 2019.
- WENGER, Etienne. Artificial intelligence and tutoring systems: computational and cognitive approaches to the communication of knowledge. Morgan Kaufmann, 1987.
- CORRELL, Nikolaus. Introduction to Autonomous Robots. 2nd Ed. Magellan Scientific, 2014.

Subárea: Segurança Computacional

Tópicos:

- 1 - Criptografia: cifragem simétrica e assimétrica; hashes; assinaturas digitais; certificados; infraestruturas de chaves públicas; técnicas avançadas de criptografia.
- 2 - Autenticação e Controle de Acesso: local; em rede; distribuída; gestão de identidades digitais; políticas de controle de acesso; modelos obrigatórios, discricionários, por papéis e por atributos; mecanismos de controle de acesso locais e distribuídos.
- 3 - Perícia Forense Computacional: padrões e ferramentas; extração de dados; manutenção da cadeia de custódia; hardware e software auxiliares; problemas abertos de PFC e desafios futuros; perícia em cloud e em memória.

4 - Segurança em sistemas e redes: filtragem de pacotes; firewalls; DMZ; ataques contra redes; segurança de protocolos/cloud/IoT/mobile; detecção de intrusão; antivírus.

5 - Mecanismos de defesa e auditoria: logs; testes de invasão; gerenciamento de vulnerabilidades e risco; testes de caixa branca e caixa preta, fuzzing.

6 - Análise de códigos: debugging para segurança; engenharia reversa; descompilação; disassembling; malware; vulnerabilidades e segurança em aplicações Web; desenvolvimento seguro.

Bibliografia:

- Ross J. Anderson. Security Engineering: A Guide to Building Dependable Distributed Systems, 2a. edição. Wiley Publishing, 2008 (disponível online).
- William Stallings. Criptografia e segurança de redes: princípios e práticas, 6a. edição. Pearson, 2015.
- Emilio Nakamura e Paulo Lício de Geus. Segurança de redes em ambientes cooperativos. Novatec, 2010.
- Michael T. Goodrich e Roberto Tamassia. Introdução à Segurança de Computadores. Bookman, 2013.
- David Kim e Michael G. Solomon. Fundamentos de segurança de sistemas de informação. LTC, 2014.
- Mark Stamp e N. J. Hoboken. Information Security: Principles and Practice. Wiley-Interscience, 2006.
- Matt Bishop. Computer Security: Art and Science. Addison-Wesley Professional, 2005.
- A. Menezes, P. van Oorschot, S. Vanstone. Handbook of Applied Cryptography. CRC Press, 2001.
- D. Andriess. Practical Binary Analysis. No Starch Press, 2018.
- D. R. Hayes. Practical Guide to Computer Forensics Investigations. Pearson, 2014.
- B. Dang, A. Gazet, E. Bachaalany, S. Josse. Practical Reverse Engineering: x86, x64, ARM, Windows Kernel, Reversing Tools, and Obfuscation. Wiley, 2014.
- P. Yaworski. Real World Bug Hunting. No Starch Press, 2019.
- G. Weidman. Penetration Testing. No Starch Press, 2014.
- B. Schneier. Applied Cryptography. Wiley, 1996.



Documento assinado eletronicamente por **FABIANO SILVA, CHEFE DO DEPARTAMENTO DE INFORMATICA - ET**, em 16/12/2020, às 09:29, conforme art. 1º, III, "b", da Lei 11.419/2006.



A autenticidade do documento pode ser conferida [aqui](#) informando o código verificador **3208647** e o código CRC **0715E52B**.