⟨**Information, Computer, [Wireless] Network,** *whatever your degree program calls this class*⟩ **security (Nicola Laurenti)**
Proposals for the literary review essay, 2017–18

Below you find a few possible topics for your literary review essay, together with a starting list of bibliographic references. The final title of your essay may be more focused on particular aspects, as some of the topics are too broad and general to be treated thoroughly. Similarly, the starting reference list should only be viewed as a suggested introduction to the topic, you are not required to follow it strictly, and it may be necessary for you to expand it.

Topic	**Anonymity measures**
Prime reference	K. Chatzikokolakis, C. Palamidessi, and P. Panangaden, "Anonymity protocols as noisy channels," *Information and Computation*, vol. 206, n. 2–4, pp. 378–401, February 2008. http://linkinghub.elsevier.com/retrieve/pii/S0890540107001241
Starting references	D. Rebollo-Monedero, J. Parra-Arnau, C. Diaz, and J. Forné, "On the Measurement of Privacy as an Attacker's Estimation Error," *ArXiv*, article ID 1111.3567, 15 November 2011. http://arxiv.org/abs/1111.3567 M. S. Alvim, K. Chatzikokolakis, P. Degano, and C. Palamidessi, "Differential Privacy versus Quantitative Information Flow," *ArXiv*, article ID 1012.4250, 20 December 2010. http://arxiv.org/abs/1012.4250 F. Sivrikaya, M. Edman, and B. Yener, "A Combinatorial Approach to Measuring Anonymity," *IEEE Intelligence and Security Informatics, 2007*, pp. 356–363. http://ieeexplore.ieee.org/document/4258723 A. Serjantov and G. Danezis, "Towards an Information Theoretic Metric for Anonymity," *Workshop on Privacy Enhancing Technologies, PET*, pp. 41–53, 2002. http://www.springerlink.com/index/10.1007/3-540-36467-6_4 W. Wang, L. Ying, and J. Zhang, "On the Relation Between Identifiability, Differential Privacy and Mutual-Information Privacy," *ArXiv*, article ID 1402.3757, 10 February 2014. http://arxiv.org/abs/1402.3757

Topic	**Blockchains beyond Bitcoin**
Prime reference	K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," *IEEE Access*, vol. 4, n. 1, pp. 2292–2303, May 2016. 7467408
Starting references	F. Buccafurri, G. Lax, S. Nicolazzo, and A. Nocera, "Overcoming Limits of Blockchain for IoT Applications," *Proceedings of the 12th International Conference on Availability, Reliability and Security, ARES '17*, 29 August – 1 September 2017, pp. 1–6. http://dl.acm.org/citation.cfm?id=3098954.3098983 A. Gervais, G. O. Karame, K. Wst, V. Glykantzis, H. Ritzdorf, and S. Capkun, "On the Security and Performance of Proof of Work Blockchains," *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security - CCS'16*, 24–28 October 2016, pp. 3–16. http://dl.acm.org/citation.cfm?id=2976749.2978341 M. Conoscenti, A. Vetro, and J. C. De Martin, "Blockchain for the Internet of Things: A systematic literature review," *2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA)'16*, 29 November – 2 December 2016, pp. 1–6. http://ieeexplore.ieee.org/document/7945805 A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts," *2016 IEEE Symposium on Security and Privacy, SP '16*, 22–26 May 2016, pp. 839–858. http://ieeexplore.ieee.org/document/7546538 G. Zyskind, O. Nathan, and A. Sandy Pentland, "Decentralizing Privacy: Using Blockchain to Protect Personal Data," *2015 IEEE Security and Privacy Workshops, SPW '15*, 21–22 May 2015, pp. 180–184. http://ieeexplore.ieee.org/document/7163223

Topic	**Efficient authentication in sensor networks**
Prime reference	L. Buttyan and J. Hubaux, *Security and cooperation in wireless networks. Thwarting malicious and selfish behavior in the age of ubiquitous computing*, Cambridge University Press, 2007, Cap. 5. http://secowinet.epfl.ch/
Starting references	A. Perrig, R. Canetti, J. Tygar, and D. Song, "Efficient authentication and signing of multicast streams over lossy channels," *IEEE Symposium on Security and Privacy. S&P 2000*, pp. 56–73. http://ieeexplore.ieee.org/document/848446 K. Hoeper and G. Gong, "Pre-Authentication and Authentication Models in Ad Hoc Networks," *Wireless Network Security*, Y. Xiao, X. Shen, D. Du eds., Boston, MA: Springer US, 2007, pp. 65–82. http://www.springerlink.com/index/10.1007/978-0-387-33112-6

Topic	**Composable security**
Prime reference	R. Canetti, "Universally composable security: a new paradigm for cryptographic protocols," *IEEE International Conference on Cluster Computing, SFCS'01*, 8–11 October 2001, pp. 136–145. http://ieeexplore.ieee.org/document/959888
Starting references	R. Canetti, "Universally composable signature, certification, and authentication," *IEEE Computer Security Foundations Workshop, CSFW'04*, 28–30 June 2004, cp(219-233). http://ieeexplore.ieee.org/document/1310743 U. M. Maurer and R. Renner, "Abstract Cryptography," *Symposium in Innovations in Computer Science, ICS'11*, 7–9 January 2011, pp. 1–21. ftp://ftp.inf.ethz.ch/pub/crypto/publications/MauRen11.pdf C. Brzuska, M. Fischlin, N. P. Smart, B. Warinschi, and S. Williams, "Less is More: Relaxed yet Composable Security Notions for Key Exchange," *Cryptology ePrint archive*, n. 242/12. https://eprint.iacr.org/2012/242

Topic	**Covert channels**
Prime reference	S. Wendzel, S. Zander, B. Fechner, and C. Herdin, "Pattern-Based Survey and Categorization of Network Covert Channel Techniques," *ACM Computing Surveys*, vol. 47, n. 3, pp. 1–26, April 2015. http://dl.acm.org/citation.cfm?id=2737799.2684195
Starting references	I.S. Moskowitz, R.E. Newman, D.P. Crepeau, A.R. Miller, "Covert channels and anonymizing networks," *ACM Workshop on Privacy in the Electronic Society, WPES 2003*, pp. 79–88. http://dl.acm.org/citation.cfm?id=1005140.1005153 K. Borders, A. Prakash, "Quantifying Information Leaks in Outbound Web Traffic," *IEEE Symposium on Security and Privacy, SP 2009*, pp. 129–140. http://ieeexplore.ieee.org/document/5207641 J. Giles, B. Hajek, "An information-theoretic and game-theoretic study of timing channels," *IEEE Transactions on Information Theory*, vol. 48, n. 9, pp. 2455–2477, September 2002. http://ieeexplore.ieee.org/document/1027777 T. He, L. Tong, "Detection of Information Flows," *IEEE Transactions on Information Theory*, vol. 54, n. 11, pp. 4925–4945, November 2008. http://ieeexplore.ieee.org/document/4655453

Topic	**Cryptanalysis of DES**
Prime reference	W. Diffie and M.E. Hellman, “Exhaustive Cryptanalysis of the NBS Data Encryption Standard,” *Computer*, vol. 10, n. 6, pp. 74–84, June 1977. http://ieeexplore.ieee.org/document/1646525
Starting references	E. Biham and A. Shamir, “Differential Cryptanalysis of the Full 16-round DES,” *Advances in Cryptology, EUROCRYPT 1993*, pp. 487–496. http://dsns.csie.nctu.edu.tw/research/crypto/HTML/PDF/C92/487.PDF E. Biham and A. Shamir, “Differential Cryptanalysis of DES-like Cryptosystems,” *Advances in Cryptology, EUROCRYPT 1990*, pp. 2–21. http://dsns.csie.nctu.edu.tw/research/crypto/HTML/PDF/C90/2.PDF M. Matsui, “Linear Cryptanalysis Method for DES Cipher,” *Advances in Cryptology, EUROCRYPT 1993*, pp. 386–397. http://www.cs.bgu.ac.il/~crp091/wiki.files/Matsui.pdf

Topic	**Distance bounding protocols**
Prime reference	I. Boureanu and S. Vaudenay, “Challenges in Distance Bounding,” *IEEE Security & Privacy Magazine*, vol. 13, n. 1, pp. 41–48, January 2015. http://ieeexplore.ieee.org/document/7031828
Starting references	E. Pagnin, G. Hancke, and A. Mitrokotsa, “Using Distance-Bounding Protocols to Securely Verify the Proximity of Two-Hop Neighbours,” *IEEE Communications Letters*, vol. 19, n. 7, pp. 1173–1176, July 2015. http://ieeexplore.ieee.org/document/7109841 A. Ranganathan, B. Danev, and S. Capkun, “Low-power Distance Bounding,” *ArXiv*, article ID 1404.4435, 17 April 2014. http://arxiv.org/abs/1404.4435 R. Trujillo-Rasua, B. Martin, and G. Avoine, “Distance Bounding Facing Both Mafia and Distance Frauds,” *IEEE Transactions on Wireless Communications*, vol. 13, n. 10, pp. 5690–5698, October 2014. 6815687 J. T. Chiang, J. J. Haas, J. Choi, and Y.-C. Hu, “Secure Location Verification Using Simultaneous Multilateration,” *IEEE Transactions on Wireless Communications*, vol. 11, n. 2, pp. 584–591, February 2012. 6108305

Topic	**Information theoretic model of authentication**
Prime reference	U.M. Maurer, “Authentication Theory and Hypothesis Testing,” *IEEE Transactions on Information Theory*, vol. 46, n. 4, pp. 1350–1356, July 2000. http://ieeexplore.ieee.org/document/850674
Starting references	L. Lai, H. El Gamal, H.V. Poor, “Authentication over Noisy Channels,” *IEEE Transactions on Information Theory*, vol. 55, n. 2, pp. 906–916, February 2009. http://ieeexplore.ieee.org/document/4777632 E. Martinian, G.W. Wornell, B. Chen, “Authentication With Distortion Criteria,” *IEEE Transactions on Information Theory*, vol. 51, n. 7, pp. 2523–2542, July 2005. http://ieeexplore.ieee.org/document/1459056

Topic	**Intrusion detection in wireless networks**
Prime reference	T. Anantvalee, J. Wu, “A Survey on Intrusion Detection in Mobile Ad Hoc Networks,” *Wireless Network Security*, Y. Xiao, X. Shen, D. Du eds., Boston, MA: Springer US, 2007, pp. 159–180. http://www.springerlink.com/index/10.1007/978-0-387-33112-6
Starting references	B. Sun, Y. Xiao, and K. Wu, “Intrusion detection in cellular mobile networks,” *Wireless Network Security*, Y. Xiao, X. Shen, D. Du eds., Boston, MA: Springer US, 2007, pp. 183–210. http://www.springerlink.com/index/10.1007/978-0-387-33112-6

Topic	**Location privacy measures**
Prime reference	M. E. Andrs, N. E. Bordenabe, K. Chatzikokolakis, and C. Palamidessi, "Geo-indistinguishability: differential privacy for location-based systems," *ACM SIGSAC Conference on Computer & Communications Security, CCS*, 4–8 November 2013, pp. 901–914. http://dl.acm.org/citation.cfm?id=2508859.2516735
Starting references	Z. Montazeri, A. Houmansadr, and H. Pishro-Nik, "Achieving Perfect Location Privacy in Wireless Devices Using Anonymization," *ArXiv*, article ID 1610.05210, 20 January 2017. http://arxiv.org/abs/http://arxiv.org/abs/1610.05210 S. Oya, C. Troncoso, and F. Prez-Gonzlez, "Is Geo-Indistinguishability What You Are Looking for?," *ArXiv*, article ID 1709.06318, 19 September 2017. http://arxiv.org/abs/http://arxiv.org/abs/1709.06318 V. Primault, S. Ben Mokhtar, C. Lauradoux, and L. Brunie, "Differentially Private Location Privacy in Practice," *ArXiv*, article ID 1410.7744, 28 October 2014. http://arxiv.org/abs/1410.7744

Topic	**Location privacy protocols**
Prime reference	T. Whalen, "Mobile Devices and Location Privacy: Where Do We Go from Here?," *IEEE Security & Privacy Magazine*, vol. 9, n. 6, pp. 61–62, November 2011. http://ieeexplore.ieee.org/document/6096615
Starting references	T. Jiang, H. J. Wang, and Y.-C. Hu, "Preserving location privacy in wireless lans," *International conference on Mobile systems, applications and services, MobiSys*, 11–13 June 2007, pp. 246–257. http://dl.acm.org/citation.cfm?id=1247660.1247689 A. Haghnegahdar, M. Khabbazian, and V. K. Bhargava, "Privacy Risks in Publishing Mobile Device Trajectories," *IEEE Wireless Communications Letters*, vol. 3, n. 3, pp. 241–244, June 2014. http://ieeexplore.ieee.org/document/6742714 J. D. Roth, M. Tummala, J. C. McEachen, and J. W. Scrofani, "On Location Privacy in LTE Networks," *IEEE Transactions on Information Forensics and Security*, vol. 12, n. 6, pp. 1358–1368, June 2017. http://ieeexplore.ieee.org/document/7828017 J. Lim, H. Yu, K. Kim, M. Kim, and S.-B. Lee, "Preserving Location Privacy of Connected Vehicles With Highly Accurate Location Updates," *IEEE Communications Letters*, vol. 21, n. 3, pp. 540–543, March 2017. 7779070 K. Shin, X. Ju, Z. Chen, and X. Hu, "Privacy protection for users of location-based services," *IEEE Wireless Communications*, vol. 19, n. 2, pp. 30–39, February 2012. http://ieeexplore.ieee.org/document/6155874

Topic	**The Meltdown and Spectre vulnerabilities on Intel, AMD and ARM processors**
Prime reference	P. Kocher et al., "Spectre Attacks: Exploiting Speculative Execution," *ArXiv*, article ID 1801.01203, 3 January 2018. http://arxiv.org/abs/1801.01203
Starting references	M. Lipp et al., "Meltdown," *ArXiv*, article ID 1801.01207, 3 January 2018. http://arxiv.org/abs/1801.01207

Topic	**Mutual information jamming games**
Prime reference	T. Basar, Y.-W. Wu, “A complete characterization of minimax and maximin encoder-decoder policies for communication channels with incomplete statistical description,” *IEEE Transactions on Information Theory*, vol. 31, n. 4, pp. 482–489, July 1985. http://ieeexplore.ieee.org/document/1057076
Starting references	G.T. Amariucai and W. Shuangqing, “Jamming Games in Fast-Fading Wireless Channels,” *Proceedings of 2008 IEEE Global Telecommunications Conference, GLOBECOM ‘08*, pp. 1–5. http://ieeexplore.ieee.org/document/4698680 A. Kashyap, T. Basar, and R. Srikant, “Correlated Jamming on MIMO Gaussian Fading Channels,” *IEEE Transactions on Information Theory*, vol. 50, n. 9, pp. 2119–2123, September 2004. http://ieeexplore.ieee.org/document/1327811 E.A. Jorswieck, H. Boche, and M. Weckerle, “Optimal Transmitter and Jamming Strategies in Gaussian MIMO Channels,” *Proceedings of Spring 2005 IEEE Vehicular Technology Conference, VTC ‘05-Spring*, pp. 978–982. http://ieeexplore.ieee.org/document/1543452 S. Ray, P. Moulin, and M. Medard, “On Optimal Signaling and Jamming Strategies in Wideband Fading Channels,” *IEEE Workshop on Signal Processing Advances for Wireless Communications, SPAWC 2006*, pp. 1–5. http://ieeexplore.ieee.org/document/4153960

Topic	**Key management for sensor networks**
Prime reference	V.K. Rayi, “Key Management Schemes in Sensor Networks,” *Wireless Network Security*, Y. Xiao, X. Shen, D. Du eds., Boston, MA: Springer US, 2007, pp. 341–380. http://www.springerlink.com/index/10.1007/978-0-387-33112-6
Starting references	Y. Wang, B. Ramamurthy, Y. Xue, “A Key Management Protocol for Wireless Sensor Networks with Multiple Base Stations,” *Proceedings of 2008 IEEE International Conference on Communications, ICC ‘08*, pp. 1625–1629. http://ieeexplore.ieee.org/document/4533350 E.K. Wang, L.C. Hui, S.M. Yiu, “A new key establishment scheme for wireless sensor networks,” *International Journal of Network Security & Its Applications*, vol. 1, pp. 17–27, 2009. http://arxiv.org/abs/1004.0591 A. Parakh, S. Kak, “A Key Distribution Scheme for Sensor Networks Using Structured Graphs,” *ArXiv*, article ID 1001.1936. http://arxiv.org/abs/1001.1936

Topic	**Physical layer secrecy for fading channels**
Prime reference	P.K. Gopala, L. Lai, and H. El Gamal, “On the Secrecy Capacity of Fading Channels,” *IEEE Transactions on Information Theory*, vol. 54, n. 10, pp. 4687–4698, October 2008. http://ieeexplore.ieee.org/document/4626059
Starting references	A. Khisti, A. Tchamkerten, and G.W. Wornell, “Secure Broadcasting Over Fading Channels,” *IEEE Transactions on Information Theory*, vol. 54, n. 6, pp. 2453–2469, June 2008. http://ieeexplore.ieee.org/document/4529277 Y. Liang, H.V. Poor, and S. Shamai (Shitz), “Secure Communication Over Fading Channels,” *IEEE Transactions on Information Theory*, vol. 54, n. 6, pp. 2470–2492, June 2008. http://ieeexplore.ieee.org/document/4529282

Topic	**Probabilistic public key cryptography**
Prime reference	A.J. Menezes, P.C. Oorschot, and S.A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996, par. 8.7. http://www.cacr.math.uwaterloo.ca/hac/about/chap8.pdf
Starting references	S. Goldwasser and S. Micali, "Probabilistic Encryption," *Journal of Computer and System Sciences*, vol. 28, n. 2, pp. 270–299, April 1984. http://groups.csail.mit.edu/cis/pubs/shafi/1984-jcss.pdf M. Blum and S. Goldwasser, "An efficient probabilistic public key encryption scheme which hides all partial information," *Advances in Cryptology, EUROCRYPT 1984*, pp. 289–299. ftp://ftp.zedz.net/pub/mirrors/AdvancesinCryptology/HTML/PDF/C84/289.PDF

Topic	**Quantum key distribution**
Prime reference	N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Reviews of Modern Physics*, vol. 74, n. 1, pp. 145–195, January 2002. http://link.aps.org/doi/10.1103/RevModPhys.74.145
Starting references	V. Scarani and C. Kurtsiefer, "The black paper of quantum cryptography: real implementation problems," *ArXiv*, article ID 0906.4547, 24 June 2009. http://arxiv.org/abs/0906.4547 R. Alleaume, J. Bouda, C. Branciard, T. Debuisschert, M. Dianati, N. Gisin, M. Godfrey, P. Grangier, T. Langer, A. Leverrier, N. Lutkenhaus, P. Painchault, M. Peev, A. Poppe, T. Pornin, J. Rarity, R. Renner, G. Ribordy, M. Riguidel, L. Salvail, A. Shields, H. Weinfurter, and A. Zeilinger, "SECOQC White Paper on Quantum Key Distribution and Cryptography," *ArXiv*, article ID quant-ph/0701168, 23 January 2007. http://arxiv.org/abs/quant-ph/0701168 A. Mink, S. Frankel, R. Perlner, "Quantum Key Distribution (QKD) and Commodity Security Protocols: Introduction and Integration," *International Journal of Network Security & Its Applications*, vol. 1, n. 2, pp. 101–112, July 2009. http://arxiv.org/abs/1004.0605

Topic	**Secret sharing**
Prime reference	A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, n. 11, pp. 612–613, November 1979. http://dl.acm.org/citation.cfm?id=359168.359176
Starting references	K. R. Sahasranand, N. Nagaraj, and S. Rajan, "How not to share a set of secrets," *ArXiv*, article ID 1001.1877, 12 January 2010. http://arxiv.org/abs/1001.1877 O. Farras, C. Padro, "Ideal Hierarchical Secret Sharing Schemes," *IEEE Transactions on Information Theory*, vol. 58, n. 5, pp. 3273–3286, May 2012. http://ieeexplore.ieee.org/document/6138912 K. Peng, "Critical survey of existing publicly verifiable secret sharing schemes," *IET Information Security*, vol. 6, n. 4, pp. 249–257, April 2012. http://ieeexplore.ieee.org/document/6404332 M. Iwamoto, "A Weak Security Notion for Visual Secret Sharing Schemes," *IEEE Transactions on Information Forensics and Security*, vol. 7, n. 2, pp. 372–382, May 2012. http://ieeexplore.ieee.org/document/6036174

Topic	**Secure data aggregation in wireless sensor networks**
Prime reference	D. Wagner, "Resilient aggregation in sensor networks," *2004 ACM workshop on Security of ad hoc and sensor networks, SASN'04*, 25 October 2004, cp(78-87). http://dl.acm.org/citation.cfm?id=1029102.1029116
Starting references	B. Przydatek, D. Song, and A. Perrig, "SIA: Secure Information Aggregation in Sensor Networks," *2003 Proceedings of the first international conference on Embedded networked sensor systems - SenSys 03'03*, 05 November 2003, cp(255). http://dl.acm.org/citation.cfm?id=958491.958521 M. Rezvani, A. Ignjatovic, E. Bertino, and S. Jha, "Secure Data Aggregation Technique for Wireless Sensor Networks in the Presence of Collusion Attacks," *IEEE Transactions on Dependable and Secure Computing*, vol. 12, n. 1, pp. 98–110, January 2015. http://ieeexplore.ieee.org/document/6786996 S. Roy, M. Conti, S. Setia, and S. Jajodia, "Secure Data Aggregation in Wireless Sensor Networks," *IEEE Transactions on Information Forensics and Security*, vol. 7, n. 3, pp. 1040–1052, June 2012. http://ieeexplore.ieee.org/document/6163407

Topic	**Secure network coding**
Prime reference	L. Lima, J. P. Vilela, P. F. Oliveira, and J. Barros, "Network Coding Security: Attacks and Countermeasures," *ArXiv*, article ID 0809.1366, 1 September 2008. http://arxiv.org/abs/0809.1366
Starting references	S. Jaggi, M. Langberg, S. Katti, T. Ho, D. Katabi, M. Medard, M. Effros, "Resilient Network Coding in the Presence of Byzantine Adversaries," *IEEE Transactions on Information Theory*, vol. 54, n. 6, pp. 2596–2603, June 2008. http://ieeexplore.ieee.org/document/4529276 D. Silva, F.R. Kschischang, "Universal Secure Error-Correcting Schemes for Network Coding," *ArXiv*, article ID 1001.3387, 19 January 2010. http://arxiv.org/abs/1001.3387 N. Cai and R. W. Yeung, "Secure Network Coding on a Wiretap Network," *IEEE Transactions on Information Theory*, vol. 57, n. 1, pp. 424–435, January 2011. http://ieeexplore.ieee.org/document/5673688

Topic	**Secure routing in ad hoc networks**
Prime reference	L. Buttyan and J. Hubaux, *Security and cooperation in wireless networks. Thwarting malicious and selfish behavior in the age of ubiquitous computing*, Cambridge University Press, 2007, Cap. 7. http://secowinet.epfl.ch/
Starting references	Y. Hu, A. Perrig, "A survey of secure wireless ad hoc routing," *IEEE Security & Privacy Magazine*, vol. 2, n. 3, pp. 28–39, May 2004. http://ieeexplore.ieee.org/document/1306970 V.C. Giruka, M. Singhal, "Secure Routing in Wireless Ad-Hoc Networks," *Wireless Network Security*, Y. Xiao, X. Shen, D. Du eds., Boston, MA: Springer US, 2007, pp. 137–158. http://www.springerlink.com/index/10.1007/978-0-387-33112-6 X. Su, Y. Xiao, R.V. Boppana, "Secure routing in ad hoc and sensor networks," *Wireless Network Security*, Y. Xiao, X. Shen, D. Du eds., Boston, MA: Springer US, 2007, pp. 381–402. http://www.springerlink.com/index/10.1007/978-0-387-33112-6 N. Marchang, and R. Datta, "Light-weight trust-based routing protocol for mobile ad hoc networks," *IET Information Security*, vol. 6, n. 2, pp. 77–ff., April 2012. http://ieeexplore.ieee.org/document/6230815 Z. Wan, K. Ren, and M. Gu, "USOR: An Unobservable Secure On-Demand Routing Protocol for Mobile Ad Hoc Networks," *IEEE Transactions on Wireless Communications*, vol. 11, n. 5, pp. 1922–1932, May 2012. http://ieeexplore.ieee.org/document/6166340

Topic	**Security in the Internet of Things**
Prime reference	J. Granjal, E. Monteiro, and J. Sa Silva, “Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues,” *IEEE Communications Surveys & Tutorials*, vol. 17, n. 3, pp. 1294–1312, January 2015. http://ieeexplore.ieee.org/document/7005393
Starting references	J. Zhou, Z. Cao, X. Dong, and A. V. Vasilakos, “Security and Privacy for Cloud-Based IoT: Challenges,” *IEEE Communications Magazine*, vol. 55, n. 1, pp. 26–33, January 2017. http://ieeexplore.ieee.org/document/7823334 R. Hummen, J. Hiller, H. Wirtz, M. Henze, H. Shafagh, and K. Wehrle, “6LoWPAN fragmentation attacks and mitigation mechanisms,” *ACM conference on security and privacy in wireless and mobile networks, WiSec*, 17–19 April 2013, pp. 55–66. http://dl.acm.org/citation.cfm?id=2462096.2462107 W. Trappe, R. Howard, and R. S. Moore, “Low-Energy Security: Limits and Opportunities in the Internet of Things,” *IEEE Security & Privacy*, vol. 13, n. 1, pp. 14–21, January 2015. http://ieeexplore.ieee.org/document/7031838

Topic	**Universal hashing functions**
Prime reference	M. N. Wegman and J. L. Carter, “New hash functions and their use in authentication and set equality,” *Journal of Computer and System Sciences*, vol. 22, n. 3, pp. 265–279, June 1981. http://linkinghub.elsevier.com/retrieve/pii/0022000081900337
Starting references	H. Krawczyk, “LFSR-based hashing and authentication,” *Advances in Cryptology, CRYPTO’94*, pp. 129–139, 1994. http://www.springerlink.com/index/T08MQA4KCJPB9K65.pdf M. Atici and D. R. Stinson, “Universal hashing and multiple authentication,” *Advances in Cryptology, CRYPTO’96*, pp. 16–30, 1996. http://www.springerlink.com/index/v48tww3t86nyug35.pdf C. Portmann, “Key recycling in authentication,” *ArXiv*, article ID 1202.1229, 6 February 2012. http://arxiv.org/abs/1202.1229

Topic	**Variations and extensions on the Shannon secrecy system**
Prime reference	M.E. Hellman, “An extension of the Shannon theory approach to cryptography ,” *IEEE Transactions on Information Theory*, vol. 23, n. 3, pp. 289–294, May 1977. http://ieeexplore.ieee.org/document/1055709
Starting references	N. Merhav and E. Arikan, “The Shannon cipher system with a guessing wiretapper,” *IEEE Transactions on Information Theory*, vol. 45, n. 6, pp. 1860–1866, June 1999. http://ieeexplore.ieee.org/document/782106 N. Merhav, “On the Shannon cipher system with a capacity-limited key-distribution channel,” *IEEE Transactions on Information Theory*, vol. 52, n. 3, pp. 1269–1273, March 2006. http://ieeexplore.ieee.org/document/1603794

Topic	**Wireless fingerprinting for device identification**
Prime reference	D.C. Loh, C.Y. Cho, C.P. Tan, R.S. Lee, “Identifying unique devices through wireless fingerprinting,” *ACM conference on Wireless network security, WiSec 2008*, pp. 46–55. http://dl.acm.org/citation.cfm?id=352533.1352542
Starting references	J. Franklin, D. McCoy, P. Tabriz, V. Neagoe, J. Van Randwyk, D. Sicker, “Passive data link layer 802.11 wireless device driver fingerprinting,” *USENIX Security 2006*, pp. 167–178. http://www.usenix.org/events/sec06/tech/franklin.html V. Brik, S. Banerjee, M. Gruteser, S. Oh, “Wireless device identification with radiometric signatures,” *ACM international conference on Mobile computing and networking, MobiCom 2008*, pp. 116–127. http://dl.acm.org/citation.cfm?id=409944.1409959

Topic	**The wormhole attack on neighbour discovery in *ad hoc* networks**
Prime reference	L. Buttyan and J. Hubaux, *Security and cooperation in wireless networks. Thwarting malicious and selfish behavior in the age of ubiquitous computing*, Cambridge University Press, 2007, Cap. 6. http://secowinet.epfl.ch/
Starting references	Y. Hu, A. Perrig, D. Johnson, "Wormhole attacks in wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, n. 2, pp. 370–80, February 2006. http://ieeexplore.ieee.org/document/1589115 D. Dong, M. Li, Y. Liu, X.-Y. Li, and X. Liao, "Topological Detection on Wormholes in Wireless Ad Hoc and Sensor Networks," *IEEE/ACM Transactions on Networking*, vol. 19, n. 6, pp. 1787–1796, December 2011. http://ieeexplore.ieee.org/document/5993472 L. Hu, D. Evans, "Using Directional Antennas to Prevent Wormhole Attacks," *Network and Distributed Systems Symposium*, 4–6 February 2004. http://www.isoc.org/isoc/conferences/ndss/04/proceedings/Papers/Hu.pdf

Topic	**Zero-knowledge cryptographic protocols**
Prime reference	O. Goldreich, "Zero-Knowledge twenty years after its invention," *Electronic Colloquium on Computational Complexity, 2002*, report n. 63. http://www.eccc.uni-trier.de/report/2002/063
Starting references	O. Goldreich, S. Micali, A. Wigderson, "Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems," *Journal of the ACM*, vol. 38, n. 3, pp. 690–728, July 1991. http://dl.acm.org/citation.cfm?id=116825.116852 U. M. Maurer, "Unifying zero-knowledge proofs of knowledge," *Progress in Cryptology, AFRICACRYPT, 2009*, pp. 272–286. ftp://ftp.inf.ethz.ch/pub/crypto/publications/Maurer09.pdf D. Catalano, M. Di Raimondo, D. Fiore, and M. Messina, "Zero-Knowledge Sets With Short Proofs," *IEEE Transactions on Information Theory*, vol. 57, n. 4, pp. 2488–2502, April 2011. http://ieeexplore.ieee.org/document/5730568