Chunlei Li - CV

Associate Professor, Department of Informatics, University of Bergen, Norway

chunlei.li@uib.no | https://people.uib.no/chunlei.li | Google Scholar

Research Interest

My research interests mainly lie in the design and decoding of error-correction codes, the design of sequences/signals in wireless communications, the construction and analysis of cryptographically strong functions, and the inter-connections of these areas

Working Experience

Associate Professor 05.2018 – Present
Department of Informatics, University of Bergen (UiB), Norway

Researcher 01.2017– 04.2018
Department of Informatics, UiB, Norway

Postdoc 01.2015– 12.2016
Dept. of Elec. Engi. and Computer Science, University of Stavanger (UiS), Norway

Research Fellow 11.2010– 12.2014
Department of Informatics, UiB, Norway

Research Assistant 09.2008– 08.2010
Department of Computer Science, Wuhan University, China

Research Projects

Sequences and Their Applications 07.2020 – 12.2024
8.7 MNOK, Funding Source: Research Council of Norway - IKTPLUSS *Principle Investigator*

Decentralized Identity for Federated Services 01.2021 – 12.2021
250 KNOK, Funding Source: UH-nett Vest *Key Partner*

Secure E-Healthcare Data Sharing by Blockchain Technology 01.2018 – 03.2019
150 KNOK, Funding Source: UH-nett Vest *Principle Investigator*

Modern Methods and Tools for Theoretical and Applied Cryptography 07.2015 – 06.2021
23.1 MNOK, Funding Source: Research Council of Norway - IKTPLUSS *Key Member*

Secure Boolean Functions for Coding and Cryptography 06.2010 – 06.2014
10.2 MNOK, Funding Source: Research Council of Norway *Key Member*

PhD Supervision

Ermes Franch: Rank-based Cryptography 12.2019 – Present
Supervisors: Chunlei Li, Tor Helleseth, Sondre Rønjom *UiB*

Wrya K. Kadir: Decoding of Codes in Rank and Hamming Metric 03.2018 – 05.2022
Supervisors: Chunlei Li, Ferdinando Zullo *UiB*

Alessandro Budroni: Notes on Lattice-Based Cryptography 11.2017 – 09.2022
Supervisors: Igor Semaev, Qian Guo, Chunlei Li *UiB*

Dan Zhang: Design of Zero Correlation Zone Sequences 04.2017 – 08.2021
Supervisors: Matthew G. Parker, Lilya Budaghyan, Tor Helleseth, Chunlei Li *UiB*

Navid G. Bardeh: Cryptanalysis of Block Ciphers 09.2016 – 03.2020
Superviors: Søndre Ronjom, Tor Helleseth, Chunlei Li *UiB*

Bo Sun: Classification of APN functions 08.2016 – 06.2018
Superviors: Lilya Budaghyan, Chunlei Li, Nian Li *UiB*

Jayachander Surbiryala: Security and Privacy in Cloud Storages 02.2016 – 12.2019
Superviors: Chunming Rong, Chunlei Li *UiS*

Master Supervision

Knut Mathias Gaard Storvestre 08.2021 – Present
Topic: Approximate Homomorphic Encryptions *UiB*

Vegard Kjørberg 06.2021 – Present
Topic: Blockchain-based ID Management *UiB*

Kristoffer Nilsen 12.2020 – 07.2022
Topic: Searchable Encryption for Secure Cloud Storage *UiB*

Kristian Wøhlk Jensen 12.2020 – 08.2022
Topic: LDPC Codes and Polar Codes for 5G communications *UiB*

Halvard Barstad 12.2019 – 07.2021
Topic: De-anonymizating Communications on TOR Networks with Deep Learning *UiB*

Ola Andreas Storstein, 12.2019 – 05.2021
Topic: On Decoding of Rank Metric Code *UiB*

Erlend Bøhler Nærbør 12.2019 – 07.2021
Topic: Penetration Testing on Web Applications *UiB*

Kjell-Erik Marstein 12.2017 – 06.2019
Topic: Improving Auditing and Privacy of EHRs by Blockchain Technology *UiB*

Morten Stangeland Salte 02.2015 – 06.2016
Topic: Secure Sharing System with Proxy Re-Encryption (co-supervision) *UiS*

Professional Services

Program Co-Chair

- International Workshop on Sequences and Their Applications, Digital, Sept. 22-25, 2020
- International Workshop on Mathematical Methods for Cryptography, Lofoten, Norway, Sept. 04-08, 2017

Program Committee

- IEEE Information Theory Workshop (ITW), Saint-Malo, April 23-28, 2023
- International Workshop on Boolean Functions and their Applications (BFA)
  - BFA-2022, Balestrand, Norway, Sept. 11-16, 2022
  - BFA-2021, Rosendal, Norway, Sept. 06-10, 2021
  - BFA-2020, Loen, Norway, Sept. 14-18, 2020
- International Workshop on Coding and Cryptography (WCC), Online, March 7 - 11, 2022
- International Workshop on Signal Design and its Application (IWSDA)
  - IWSDA-2021, Aug. 2-6, 2021, Colchester, UK
  - IWSDA-2019, Oct. 20-24, 2019, GuangDong, China
- International Workshop on SEquences and Their Applications, Hongkong, China, Oct. 01-06, 2018
- International Workshop on the Arithmetic of Finite Fields, Bergen, Norway, June 14-16, 2018
- International Workshop on Resource Brokering with blockchain (RBChain)
  - RBChain-2019, Dec. 10, 2019, Sydney, Australia
  - RBChain-2018, Dec. 10, 2018, Nicosia, Cyprus
- Norwegian Information Security Conference (NISK)
  - NISK2020, Nov. 23-25, 2020, Oslo, Norway
  - NISK2019, Nov. 25-27, 2019, Narvik, Norway
  - NISK2018, Sept. 19-20, 2018, Longyearbyen, Norway

  - NISK2017, Nov. 27-29, 2017, Oslo, Norway
  - NISK2016, Nov. 28-30, 2016, Bergen, Norway
  - NISK2015, Nov. 23-25, 2015, Ålesund, Norway

Organizing Committee

- International Workshop on Boolean Functions and their Applications (BFA)
  - BFA-2020, Sept. 14-18, Loen, Norway
  - BFA-2018, June 17-22, Loen, Norway
  - BFA-2017, July 3-8, 2017, Os, Norway
- International Workshop on the Arithmetic of Finite Fields (WAIFI)
  - WAIFI-2018: June 14-16, Bergen, Norway

Guest Editor

- Editorial: Special Issue on Mathematical Methods for Cryptography. Cryptogr. Commun. 11(3), (2019)
- Editorial: Special Issue on SEquences and Their Applications. Cryptogr. Commun., 2021

Peer Review (publons.com)

- IEEE Transaction on Information Theory
- IEEE Transaction on Communications
- IEEE Transaction on Cloud Computing
- Design, Codes and Crytography
- Crytography and Communications
- Finite Fields and Their Applications

Faculty Service

PhD Thesis Evaluation

- Leader of Evaluation Committee for *Albin Severinson*, Simula-UiB — 09.2022
  Thesis: Straggler-Resilient Distributed Computing
- Leader of Evaluation Committee for *Isaac Andrés Canales Martínez*, UiB — 03.2022
  Thesis: On Properties of Bent and Almost Perfect Nonlinear Functions
- Leader of Evaluation Committee for *John Petter Indry*, Simula-UiB — 10.2021
  Thesis: Selected Topics in Cryptanalysis of Symmetric Ciphers
- Leader of Evaluation Committee for *Diana Davidova*, UiB — 09.2021
  Thesis: On Properties of Bent and Almost Perfect Nonlinear Functions
- Leader of Evaluation Committee for *Irene Villa*, UiB — 06.2020
  Thesis: Analysis, Classification and Construction of Optimal Cryptographic Boolean Functions
- Member of Evaluation Committee - Mid-term evaluation of Anton Tkachenco, HVL, — 03.2020

PhD Defence

- Leader of PhD Defence - Sachin Jayesh Valera, UiB, — 08-2021
- Leader of PhD Defence - Katarzyna Chyzynska, UiB, — 10-2019

Master Evaluation

- Internal Examiner - Sivanja Naguleswaran, UiB, — 06.2020
- External Examiner - Anisa Zhurda, Holme Jrgen, UiS, — 08.2020

Organization of CryptoAften1 (an educational activity) — 11.2019

Teaching

INF140 - Introduction of Cyber Security, UiB	Autumn, 2022
INF243 - Algebraic Coding, UiB	Spring, 2022
INF140 - Introduction of Cyber Security, UiB	Autumn, 2021
INF143A - Applied Cryptography, UiB	Spring, 2021
INF140 - Introduction of Cyber Security, UiB	Spring, Autumn, 2020
INF142 - Compute Networks, UiB	Spring, 2019
INF240 - Basic Codes, UiB	Autumn, 2018
DAT510 - Security and Vulnerability in Network, UiS	Autumn, 2015, 2016

Publication

[1] Kangquan Li, Yue Zhou, Chunlei Li, and Longjiang Qu. Two new families of quadratic APN functions. *IEEE Trans. Inf. Theory*, 68(7):4761–4769, 2022.

[2] Haode Yan, Yongbo Xia, Chunlei Li, Tor Helleseth, Maosheng Xiong, and Jinquan Luo. The differential spectrum of the power mapping x^{p^n-3}. *IEEE Trans. Inf. Theory*, 68(8):5535–5547, 2022.

[3] Guang Yang, Chunlei Li, and Kjell E. Marstein. A blockchain-based architecture for securing electronic health record systems. *Concurr. Comput. Pract. Exp.*, 33(14), 2021.

[4] Kangquan Li, Chunlei Li, Tor Helleseth, and Longjiang Qu. Cryptographically strong permutations from the butterfly structure. *Des. Codes Cryptogr.*, 89(4):737–761, 2021.

[5] Kangquan Li, Chunlei Li, Tor Helleseth, and Longjiang Qu. Binary linear codes with few weights from two-to-one functions. *IEEE Trans. Inf. Theory*, 67(7):4263–4275, 2021.

[6] Tor Helleseth, Daniel J. Katz, and Chunlei Li. The resolution of niho's last conjecture concerning sequences, codes, and boolean functions. *IEEE Trans. Inf. Theory*, 67(10):6952–6962, 2021.

[7] Kangquan Li, Chunlei Li, Tor Helleseth, and Longjiang Qu. A complete characterization of the APN property of a class of quadrinomials. *IEEE Trans. Inf. Theory*, 67(11):7535–7549, 2021.

[8] Zhimin Sun, Xiangyong Zeng, Chunlei Li, Yi Zhang, and Lin Yi. The expansion complexity of ultimately periodic sequences over finite fields. *IEEE Trans. Inf. Theory*, 67(11):7550–7560, 2021.

[9] Wrya K. Kadir, Chunlei Li, and Ferdinando Zullo. On interpolation-based decoding of a class of maximum rank distance codes. In *IEEE International Symposium on Information Theory, ISIT 2021, Melbourne, Australia, July 12-20, 2021*, pages 31–36. IEEE, 2021.

[10] Anne Canteaut, Lukas Kölsch, Chao Li, Chunlei Li, Kangquan Li, Longjiang Qu, and Friedrich Wiemer. Autocorrelations of vectorial boolean functions. In Patrick Longa and Carla Ràfols, editors, *Progress in Cryptology - LATINCRYPT 2021 - 7th International Conference on Cryptology and Information Security in Latin America, Bogotá, Colombia, October 6-8, 2021, Proceedings*, volume 12912 of *Lecture Notes in Computer Science*, pages 233–253. Springer, 2021.

[11] Yang Yang and Chunlei Li. New quaternary sequences with optimal odd-periodic autocorrelation magnitude. *Cryptogr. Commun.*, 12(3):363–374, 2020.

[12] Chunlei Li and Yang Yang. On three conjectures of binary sequences with low odd-periodic autocorrelation. *Cryptogr. Commun.*, 12(3):427–442, 2020.

[13] Wrya K. Kadir and Chunlei Li. On decoding additive generalized twisted gabidulin codes. *Cryptogr. Commun.*, 12(5):987–1009, 2020.

[14] Yongbo Xia, Xianglai Zhang, Chunlei Li, and Tor Helleseth. The differential spectrum of a ternary power mapping. *Finite Fields Their Appl.*, 64:101660, 2020.

[15] Lilya Budaghyan, Chunlei Li, and Matthew Geoffrey Parker. Editorial: Special issue on mathematical methods for cryptography. *Cryptogr. Commun.*, 11(3):363–365, 2019.

[16] Vladimir Edemskiy, Chunlei Li, Xiangyong Zeng, and Tor Helleseth. The linear complexity of generalized cyclotomic binary sequences of period p^n. *Des. Codes Cryptogr.*, 87(5):1183–1197, 2019.

[17] Lisha Li, Chaoyun Li, Chunlei Li, and Xiangyong Zeng. New classes of complete permutation polynomials. *Finite Fields Their Appl.*, 55:177–201, 2019.

[18] Xiaofang Xu, Chunlei Li, and Xiangyong Zeng. Nonsingular polynomials from feedback shift registers. *Int. J. Found. Comput. Sci.*, 30(3):469–487, 2019.

[19] Chunlei Li, Chunming Rong, and Martin Gilje Jaatun. A cost-efficient protocol for open blockchains. In *2019 International Conference on Cyber Security and Protection of Digital Services, Cyber Security 2018, Oxford, United Kingdom, June 3-4, 2019*, pages 1–7. IEEE, 2019.

[20] Chunlei Li. Interpolation-based decoding of nonlinear maximum rank distance codes. In *IEEE International Symposium on Information Theory, ISIT 2019, Paris, France, July 7-12, 2019*, pages 2054–2058. IEEE, 2019.

[21] Zibi Xiao, Xiangyong Zeng, Chunlei Li, and Tor Helleseth. New generalized cyclotomic binary sequences of period p^2. *Des. Codes Cryptogr.*, 86(7):1483–1497, 2018.

[22] Xiaofang Xu, Chunlei Li, Xiangyong Zeng, and Tor Helleseth. Constructions of complete permutation polynomials. *Des. Codes Cryptogr.*, 86(12):2869–2892, 2018.

[23] Ziran Tu, Xiangyong Zeng, Chunlei Li, and Tor Helleseth. A class of new permutation trinomials. *Finite Fields Their Appl.*, 50:178–195, 2018.

[24] Cunsheng Ding, Chunlei Li, and Yongbo Xia. Another generalisation of the binary reed-muller codes and its applications. *Finite Fields Their Appl.*, 53:144–174, 2018.

[25] Jinyong Shan, Lei Hu, Xiangyong Zeng, and Chunlei Li. A construction of 1-resilient boolean functions with good cryptographic properties. *J. Syst. Sci. Complex.*, 31(4):1042–1064, 2018.

[26] Guang Yang and Chunlei Li. A design of blockchain-based architecture for the security of electronic health record (EHR) systems. In *2018 IEEE International Conference on Cloud Computing Technology and Science, CloudCom 2018, Nicosia, Cyprus, December 10-13, 2018*, pages 261–265. IEEE Computer Society, 2018.

[27] Yongbo Xia and Chunlei Li. Three-weight ternary linear codes from a family of power functions. *Finite Fields Their Appl.*, 46:17–37, 2017.

[28] Adel Alahmadi, Hussain Alhazmi, Shakir Ali, Tor Helleseth, Rola Hijazi, Chunlei Li, and Patrick Solé. An analogue of the F_4-goethals code in non-primitive length. *J. Syst. Sci. Complex.*, 30(4):950–966, 2017.

[29] Zhimin Sun, Xiangyong Zeng, Chunlei Li, and Tor Helleseth. Investigations on periodic sequences with maximum nonlinear complexity. *IEEE Trans. Inf. Theory*, 63(10):6188–6198, 2017.

[30] Chunlei Li and Tor Helleseth. Quasi-perfect linear codes from planar and APN functions. *Cryptogr. Commun.*, 8(2):215–227, 2016.

[31] Cunsheng Ding, Chunlei Li, Nian Li, and Zhengchun Zhou. Three-weight cyclic codes and their weight distributions. *Discret. Math.*, 339(2):415–427, 2016.

[32] Chaoyun Li, Xiangyong Zeng, Chunlei Li, Tor Helleseth, and Ming Li. Construction of de bruijn sequences from lfsrs with reducible characteristic polynomials. *IEEE Trans. Inf. Theory*, 62(1):610–624, 2016.

[33] Xinjiao Chen, Chunlei Li, and Chunming Rong. Perfect gaussian integer sequences from cyclic difference sets. In *IEEE International Symposium on Information Theory, ISIT 2016, Barcelona, Spain, July 10-15, 2016*, pages 115–119. IEEE, 2016.

[34] Yongbo Xia, Tor Helleseth, and Chunlei Li. Some new classes of cyclic codes with three or six weights. *Adv. Math. Commun.*, 9(1):23–36, 2015.

[35] Jiao Li, Claude Carlet, Xiangyong Zeng, Chunlei Li, Lei Hu, and Jinyong Shan. Two constructions of balanced boolean functions with optimal algebraic immunity, high nonlinearity and good behavior against fast algebraic attacks. *Des. Codes Cryptogr.*, 76(2):279–305, 2015.

[36] Ziran Tu, Xiangyong Zeng, Chunlei Li, and Tor Helleseth. Permutation polynomials of the form $(x^{p^m}-x+\delta)^s+l(x)$ over the finite field $_{fp2m}$ of odd characteristic. *Finite Fields Their Appl.*, 34:20–35, 2015.

[37] Nian Li, Chunlei Li, Tor Helleseth, Cunsheng Ding, and Xiaohu Tang. Optimal ternary cyclic codes with minimum distance four and five. *Finite Fields Their Appl.*, 30:100–120, 2014.

[38] Yongbo Xia, Shaoping Chen, Tor Helleseth, and Chunlei Li. Cross-correlation between a p-ary m-sequence and its all decimated sequences for $d=((p^m+1)(p^m+p-1))/(p+1)$. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.*, 97-A(4):964–969, 2014.

[39] Chaoyun Li, Xiangyong Zeng, Tor Helleseth, Chunlei Li, and Lei Hu. The properties of a class of linear fsrs and their applications to the construction of nonlinear fsrs. *IEEE Trans. Inf. Theory*, 60(5):3052–3061, 2014.

[40] Chunlei Li, Nian Li, Tor Helleseth, and Cunsheng Ding. The weight distributions of several classes of cyclic codes from APN monomials. *IEEE Trans. Inf. Theory*, 60(8):4710–4721, 2014.

[41] Yongbo Xia, Chunlei Li, Xiangyong Zeng, and Tor Helleseth. Some results on cross-correlation distribution between a \(p\) -ary \(m\) -sequence and its decimated sequences. *IEEE Trans. Inf. Theory*, 60(11):7368–7381, 2014.

[42] Chaoyun Li, Xiangyong Zeng, Chunlei Li, and Tor Helleseth. A class of de bruijn sequences. *IEEE Trans. Inf. Theory*, 60(12):7955–7969, 2014.

[43] Jie Li, Xiangyong Zeng, Xiaohu Tang, and Chunlei Li. A family of quadriphase sequences of period 4(2 n - 1) with low correlation and large linear span. *Des. Codes Cryptogr.*, 67(1):19–35, 2013.

[44] Chunlei Li, Nian Li, and Matthew Geoffrey Parker. Complementary sequence pairs of types II and III. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.*, 95-A(11):1819–1826, 2012.

[45] Wenjie Jia, Xiangyong Zeng, Tor Helleseth, and Chunlei Li. A class of binomial bent functions over the finite fields of odd characteristic. *IEEE Trans. Inf. Theory*, 58(9):6054–6063, 2012.

[46] Chunlei Li and Tor Helleseth. New nonbinary sequence families with low correlation and large linear span. In *Proceedings of the 2012 IEEE International Symposium on Information Theory, ISIT 2012, Cambridge, MA, USA, July 1-6, 2012*, pages 1411–1415. IEEE, 2012.

[47] Guang Gong, Tor Helleseth, Honggang Hu, and Chunlei Li. New three-valued walsh transforms from decimations of helleseth-gong sequences. In Tor Helleseth and Jonathan Jedwab, editors, *Sequences and Their Applications - SETA 2012 - 7th International Conference, Waterloo, ON, Canada, June 4-8, 2012. Proceedings*, volume 7280 of *Lecture Notes in Computer Science*, pages 327–337. Springer, 2012.

[48] Huanguo Zhang, Chunlei Li, and Ming Tang. Capability of evolutionary cryptosystems against differential cryptanalysis. *Sci. China Inf. Sci.*, 54(10):1991–2000, 2011.

[49] Huanguo Zhang, Chunlei Li, and Ming Tang. Evolutionary cryptography against multidimensional linear cryptanalysis. *Sci. China Inf. Sci.*, 54(12):2565–2577, 2011.

[50] Houzhen Wang, Huanguo Zhang, Qianhong Wu, Yu Zhang, Chunlei Li, and Xinyu Zhang. Design theory and method of multivariate hash function. *Sci. China Inf. Sci.*, 53(10):1977–1987, 2010.

[51] Claude Carlet, Xiangyong Zeng, Chunlei Li, and Lei Hu. Further properties of several classes of boolean functions with optimum algebraic immunity. *Des. Codes Cryptogr.*, 52(3):303–338, 2009.