UNIVERSITATEA "AUREL VLAICU" DIN ARAD
FACULTATEA DE ŞTIINŢE EXACTE
Department of Mathematics and Computer Science | Academic Year 2026–2027

Dissertation Topics for Master's Thesis (Disertaţie)

Advanced Cryptography, Machine Learning, Data Science, and Simulation

Scientific Advisor: Vlad-Florin DRAGOI

Program Overview

Master's thesis projects demand rigorous mathematical foundations, advanced algorithmic synthesis, and empirical validation. Topics integrate state-of-the-art post-quantum cryptography, probabilistic simulation techniques, advanced Unix/Web defense, machine learning for anomaly detection, and modern coding theory.

Topic 1: Semantic Security and Random Oracle Reductions for Code-Based PKC

Specialization: Advanced Cryptography & Post-Quantum Security
Description: Achieving IND-CCA2 security without relying on Random Oracles is a major milestone in post-quantum cryptography. This research topic focuses on semantic security reductions for McEliece and Niederreiter schemes, analyzing conversions by Bellare-Rogaway, Fujisaki-Okamoto, Pointcheval, and Nojima et al.

- **Key Objectives:** Formalize security proofs in the standard model vs. random oracle model; evaluate computational overheads of strict semantic security conversions; model side-channel attack vectors.
- **Required Skills:** Provable Security, Abstract Algebra, Formal Proof Analysis, C++/SageMath.

Topic 2: Monte Carlo Simulation Techniques: Variance Reduction via Importance Sampling and Inversion Methods

Specialization: Computational Mathematics & Stochastic Simulation
Description: Efficient simulation of rare events in security networks and code distance estimations requires advanced stochastic methods. The student will research inverse transform sampling, rejection sampling, and importance sampling algorithms to minimize estimator variance in high-dimensional settings.

- **Key Objectives:** Develop optimized Importance Sampling algorithms for rare-event probability bounds; compare classical Monte Carlo with Markov Chain Monte Carlo (MCMC); apply to decoding error bounds.
- **Required Skills:** Advanced Probability Theory, Stochastic Processes, Python/R/C++.

Topic 3: Machine Learning and Data Science for Cyber Threat Intelligence and Intrusion Detection

Specialization: Data Science & Unix/Web Security
Description: Combining data science and system security enables proactive threat hunting. This project investigates machine learning algorithms (Random Forests, XGBoost, and Autoencoders) applied to high-frequency Unix system log streams (auditd/syslog) and Web Application Firewall (WAF) traffic.

- **Key Objectives:** Build an end-to-end data pipeline for log feature extraction; address heavy class imbalance in cyber attack datasets; evaluate real-time threat detection accuracy versus false positives.
- **Required Skills:** Machine Learning (Scikit-Learn, PyTorch/TensorFlow), Unix Systems, Data Processing.

Topic 4: Advanced Polar Code Construction Techniques and SCL Decoding under Quantum Channels

Specialization: Coding Theory & Information Theory
Description: Polar codes are pivotal in 5G wireless standards and post-quantum error control. This research investigates frozen bit selection algorithms (Gaussian Approximation vs. Tal & Vardy algorithm) and Successive Cancellation List (SCL) decoding with CRC aiding.

- **Key Objectives:** Implement state-of-the-art construction algorithms for arbitrary channels; model hardware complexity of SCL list sizes; compare performance against LDPC codes.
- **Required Skills:** Modern Coding Theory, Information Theory, Python/C++.

Key Academic References

References

[1] M. Bellare and P. Rogaway, "Optimal Asymmetric Encryption – How to Encrypt with RSA," in *Proc. EUROCRYPT '94*, LNCS 950, Springer, pp. 92–111, 1995.

[2] E. Fujisaki and T. Okamoto, "Secure Integration of Asymmetric and Symmetric Encryption Schemes," in *Proc. CRYPTO '99*, LNCS 1666, Springer, pp. 537–554, 1999.

[3] D. Pointcheval, "Chosen-Ciphertext Security for Any One-Way Cryptosystem," in *Proc. PKC '00*, LNCS 1751, Springer, pp. 129–146, 2000.

[4] R. Nojima, H. Imai, K. Kobara, and K. Morozov, "Semantic Security for the McEliece Cryptosystem without Random Oracles," *CiteseerX Pre-print*, 2006.

[5] P.-L. Cayrel, "Research in Code-Based Cryptography and Security," Research Portal, http://cayrel.net/?-Research-.

[6] C. P. Robert and G. Casella, *Monte Carlo Statistical Methods*, 2nd ed., Springer-Verlag, 2004.

[7] L. Devroye, *Non-Uniform Random Variate Generation*, Springer-Verlag, 1986.

[8] S. Asmussen and P. W. Glynn, *Stochastic Simulation: Algorithms and Analysis*, Springer, 2007.

[9] A. L. Buczak and E. Guven, "A Survey of Data Mining and Machine Learning Methods for Cyber Intrusion Detection," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1153–1176, 2015.

[10] R. Sommer and V. Paxson, "Outside the Closed World: On Using Machine Learning for Network Intrusion Detection," in *Proc. IEEE Symposium on Security and Privacy (S&P)*, pp. 305–316, 2010.

[11] I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*, MIT Press, 2016.

[12] E. Arikan, "Channel Polarization: A Method for Constructing Capacity-Achieving Codes for Symmetric Binary-Input Memoryless Channels," *IEEE Trans. Inf. Theory*, vol. 55, no. 7, pp. 3051–3073, 2009.

[13] I. Tal and A. Vardy, "List Decoding of Polar Codes," *IEEE Trans. Inf. Theory*, vol. 61, no. 5, pp. 2213–2226, 2015.

[14] P. Trifonov, "Efficient Design and Decoding of Polar Codes," *IEEE Trans. Commun.*, vol. 60, no. 1, pp. 22–27, 2012.

[15] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero Trust Architecture," NIST Special Publication 800-207, National Institute of Standards and Technology, 2020.

[16] M. Zalewski, "American Fuzzy Lop (AFL) Fuzzer," https://lcamtuf.coredump.cx/afl/, 2012.

[17] D. Hardt, "The OAuth 2.0 Authorization Framework," RFC 6749, IETF, 2012.