UNIVERSITÀ DI TRENTO

Fondazione Bruno Kessler – FBK

Borse di studio/ Scholarships

A	**Mathematical Analysis of Disinformation Spreading in online Social Network**

Topic: The objective of this thesis is to advance mathematical models and analytical tools for the
investigation of online social systems and their influence on the dissemination of disinformation. The study will utilise the expertise of several fields, including graph theory, statistics, and time series, to study the mechanisms of information diffusion on large social media datasets, anticipate the spreading of viral content and design countermeasures to limit the impact of unreliable news.

P.I.: GALLOTTI RICCARDO

Contacts: rgallotti@fbk.eu

Synthetic description of the activity and expected research outcome

The objective of this thesis is to advance mathematical models and analytical tools for investigating the dynamics of information spreading over online social networks and its impact on the dissemination of false or misleading news. The study will draw upon expertise from various fields, including stochastic processes, network theory, data science, artificial intelligence, and statistics, to analyze the structural and functional characteristics of social networks formed among social media users within (and potentially across) multiple social media platforms, as well as the associated dynamic processes driving the diffusion of content.

Through our research, we aim to contribute to the understanding of online communication dynamics by developing appropriate mathematical and statistical tools. Our ultimate goal is to provide insightful information to journalists, fact-checkers, and policymakers regarding the trustworthiness of specific sources of information and to assist in particular policymakers in making decisions regarding the containment of misinformation and disinformation.

To achieve these objectives, we will adopt an interdisciplinary approach that will advance our understanding of online social networks both as a mathematical model and a sociotechnical system. Our focus will be on (i) the development of mathematical models that effectively capture the complexity of online social media platforms such as Telegram, YouTube, or Twitter; (ii) the development of statistical tools to identify patterns, predict outcomes, and classify different online narratives based on their properties; (iii) the implementation of these tools on large repositories of social media data and the identification of solutions to minimize disinformation spreading.

In this third implementation phase, the project will merge traditional statistical methods with cutting-edge machine learning algorithms. The objective is to process extensive databases of online messages and extract insights on circulating content that would otherwise remain unattainable at this scale. Additionally, we will explore reinforcement learning and cooperative AI methodologies as potential solutions for developing social bots aiming to mitigate the social impact of misinformation and disinformation, ultimately striving to foster a more sustainable and efficient online environment.

References

Brody & Meier. "Mathematical models for fake news." Financial Informatics: An Information-Based Approach to Asset Pricing. 2022. 405-423.
Butts et al. "Mathematical modeling of disinformation and effectiveness of mitigation policies." Scientific Reports 13.1 (2023): 18735.
De Domenico et al. "The physics of spreading processes in multilayer networks." Nature Physics 12.10 (2016): 901-906.

Gallotti et al. "Assessing the risks of 'infodemics' in response to COVID-19 epidemics." Nature human behaviour 4.12 (2020): 1285-1293.

Ideal candidate

Master in a data-oriented field (Physics, Math, Data Science, Computer Science, Computational Social Science, …)
Software development skills (preferably in Python)
Attitude towards analytical thinking
Good knowledge and proficiency of the English language
Team working attitude
Good communication and relation skills.

UNIVERSITÀ DI TRENTO

Fondazione Bruno Kessler – FBK

Borse di studio/ Scholarships

B	**Quantum-safe cryptography for the Cloud**

Topic: Cloud service providers enable outsourcing of services such as data storage and computation. Cryptographic protocols assist data controllers in satisfying regulatory and security concerns to maximise the privacy of data subjects and minimise the impact of data breaches.
Searchable encryption [LTTMC_22] aims to enable rich queries on encrypted data, so that the data stored in the cloud may be searched over and retrieved while maintaining confidentiality at rest.
Homomorphic encryption [MSMBFA_22] aims to enable computation over encrypted data, while maintaining confidentiality in use and in output. This is a particularly appealing prospect given recent advances in machine learning [MFKBS_24].

P.I.: TOMASI ALESSANDRO

Contacts: altomasi@fbk.eu

Synthetic description of the activity and expected research outcome

While both families of protocols promise greater privacy and security, enabling scenarios such as the storage and analysis of medical records while maximising confidentiality of both the data and the results, they come at a heavy computational cost. Concretely, this research may focus on more efficient number-theoretic transforms for polynomials that are not powers of two, tighter error bounds for more efficient parameters, or tools to make FHE more accessible and transparent to developers as well as end-users. In addition, for some applications such as e-voting it is desirable to have zero-knowledge proofs of correctness of the data under computation, which remains an area of ongoing research [dPLNS_17].
The candidate is expected to analyse alternative solutions where tasks can be either entirely or partially outsourced and conduct experimental assessments, comparing the outcomes against legacy approaches in terms of performance, security, and privacy requirements.

References

[LTTMC_22] Public-key Authenticated Encryption with Keyword Search: Cryptanalysis, Enhanced Security, and Quantum-resistant Instantiation. Z-Y Liu, Y-F Tseng, R Tso, M Mambo, and Y-C Chen. ASIA CCS '22. ACM, NY, USA, 423-436. https://doi.org/10.1145/3488932.3497760 https://eprint.iacr.org/2021/1008
[MFKBS_24] Neural Network Training on Encrypted Data with TFHE. L Montero, J Frery, C Kherfallah, R Bredehoft, A Stoian, 2024. https://doi.org/10.48550/arXiv.2401.16136
[MSMBFA_22] Survey on Fully Homomorphic Encryption, Theory, and Applications. Marcolla, Sucasas, Manzano, Bassoli, Fitzek, Aaraj https://eprint.iacr.org/2022/1602
[dPLNS_17] Practical Quantum-Safe Voting from Lattices. R del Pino, V Lyubashevsky, G Neven, and G Seiler. https://eprint.iacr.org/2017/1235

Ideal candidate

MSc in Mathematics or Computer Science with a focus on Cryptography
Software development skills, preferably in Rust or Python
Good knowledge and proficiency of the English language
Expertise on one or more of the scientific topics in the call description above

UNIVERSITÀ DI TRENTO

Fondazione Bruno Kessler – FBK

Borse di studio/ Scholarships

C	Quantum-safe cryptography for privacy-enhancing digital identity

Topic: There is a strong interest in privacy-enhancing technologies to satisfy the complex requirements of digital identity. Important use cases include the European Digital Identity Wallet [EUDIW] and the Mobile Drivers' License [ISO 18013-5]. Challenging but highly significant design goals include minimizing the personal data shared at each presentation by selectively disclosing the attributes in each credential [SD-JWT], and enabling verifiers to check the status of credentials [TSL, OSA], while preventing anyone from correlating the activity of credential holders between presentations.

P.I.: TOMASI ALESSANDRO

Contacts: altomasi@fbk.eu

Synthetic description of the activity and expected research outcome

The successful candidate will carry out research on post-quantum privacy-enhancing cryptography to satisfy the complex requirements of the European Digital Identity Wallet [EUDIW]. Two groups of algorithms of particular interest are digital signatures for selective disclosure of attributes [FS+24] and accumulators to prove set (non-)membership [CL02, VB20], with the zero-knowledge proofs to generate correlation-resistant presentations. These algorithms form the basis of anonymous credential protocols, of which post-quantum variants are the topic of active research [BC+23].

References

[BC+23] O Blazy, C Chevalier, G Renaut, T Ricosset, E Sageloli, H Senet: "Efficient Implementation of a Post-Quantum Anonymous Credential Protocol". ARES 2023, ACM. doi: 10.1145/3600160.3600188
[CL02] J Camenisch, A Lysyanskaya: "Dynamic Accumulators and Application to Efficient Revocation of Anonymous Credentials." CRYPTO 2002. doi: 10.1007/3-540-45708-9_5
[EUDIW] The European Digital Identity Wallet https://github.com/eu-digital-identity-wallet
[ISO 18013-5] Personal identification - ISO-compliant driving licence - part 5: Mobile driving licence (mDL) application, 09 2021.
[FS+24] A Flamini, G Sciarretta, M Scuro, A Sharif, A Tomasi, S Ranise: "On Cryptographic Mechanisms for the Selective Disclosure of Verifiable Credentials". arXiv:2401.08196.
[LLX07] J Li, N Li, R Xue: "Universal Accumulators with Efficient Nonmembership Proofs". ACNS 2007. doi: 10.1007/978-3-540-72738-5_17
[OSA] OAuth Status Attestations https://github.com/peppelinux/draft-demarco-oauth-status-attestations
[TSL] Token Status List https://github.com/oauth-wg/draft-ietf-oauth-status-list
[SD-JWT] Selective Disclosure for JWTs (SD-JWT) https://github.com/oauth-wg/oauth-selective-disclosure-jwt
[VB20] G Vitto, A Biryukov: "Dynamic Universal Accumulator with Batch Update over Bilinear Groups". IACR 2020, CT-RSA 2022. ia.cr/2020/777, doi: 10.1007/978-3-030-95312-6_17.

Ideal candidate

MSc in Mathematics or Computer Science with a focus on Cryptography
Software development skills, preferably in Rust or Python
Good knowledge and proficiency of the English language
Expertise on one or more of the scientific topics in the call description above

UNIVERSITÀ DI TRENTO

Fondazione Bruno Kessler – FBK

Borse di studio/ Scholarships

D	**Statistical modeling of hypergraphs**

Topic: Development of generative models for hypergraphs in the life science realm, with applications on computational biology tasks.

P.I.: JURMAN GIUSEPPE

Contacts: giuseppe.jurman@fbk.eu

Synthetic description of the activity and expected research outcome

Over the past two decades a broad variety of statistical models have been developed for pairwise interactions. The latter are encoded by graphs where interacting pairs of nodes are connected by links. However, modern applications in various fields, such as metabolic, biological, brain and social networks, highlight the need to account for higher-order interactions, that is interactions involving a group of three or more nodes, e.g., [1,2]. Hypergraphs are the extension of graphs that provide the formalism for these higher-order interactions, as each hyperedge is a subset of nodes taking part in an interaction. Despite an increasing interest for these higher-order interactions, the statistical literature on this topic remains scarce. This PhD project will investigate a number of open challenges, and propose new methodologies, for the statistical modeling of hypergraphs. In particular, we will develop clustering models on hypergraphs, based on novel embeddings in a latent space [3,4]. While this will be mainly conducted for static hypergraphs, in a second part of the project, we will investigate an extension of relational event models [5] to hypergraphs, for modeling the formation of hyperedges over time. Generative models such as those described above will not only reveal the underlying structure of a hypergraph and its possible drivers, but it will also allow for the prediction of missing hyperedges.

The proposed methods will be evaluated both theoretically, e.g., by studying their consistency, and empirically, via extensive simulation studies. Implementations, e.g. in the form of R packages, will also be made available. Finally, we will consider an application of the methods to biological networks, which are better described by complexes of proteins than by pairwise protein-protein interactions.

The PhD will be co-supervised by Veronica Vinciotti (Department of Mathematics, University of Trento) and Giuseppe Jurman (Fondazione Bruno Kessler, Trento). The development clustering models will benefit from the collaboration with Prof. Catherine Matias (Sorbonne Université), while relational event moel for hypergraphs will be conducted in collaboration with Prof. Ernst Wit (Università Svizzera italiana).

References

1. Chen, C., Liao, C. and Liu, Y. (2023) Teasing out missing reactions in genome-scale metabolic networks through hypergraph learning. Nat Commun 14, 2375 https://doi.org/10.1038/s41467-023-38110-7

2. Stehlé, J. et al. (2011) High-Resolution Measurements of Face-to-Face Contact Patterns in a Primary School. PLoS ONE 6(8): e23176. https://doi.org/10.1371/journal.pone.0023176

3. Gong, X., Higham, D. and Zygalakis, K. (2023) Generative hypergraph models and spectral embedding. Sci Rep 13, 540 https://doi.org/10.1038/s41598-023-27565-9

4. Poda, V. and Matias, C. (2024) Comparison of modularity-based approaches for nodes clustering in binary hypergraphs. https://arxiv.org/abs/2401.14028
5. Butts, C. T. (2008) A Relational Event Framework for Social Action. Sociological Methodology 38(1), 155-200 https://doi.org/10.1111/j.1467-9531.2008.00203.x

Ideal candidate

The ideal candidate should hold a Master's degree in Mathematics, Statistics, or a related field. They must have a solid understanding of graph theory and hypergraphs, evidenced by previous academic or project involvement relevant to this project's focus. Proficiency in programming languages such as Python and R is essential. Knowledge of biological networks and experience with deep learning algorithms, while not essential, will be considered a plus. We are seeking a motivated independent researcher eager to work in a team within a multidisciplinary field.

UNIVERSITÀ DI TRENTO

Dipartimento di Matematica – Università di Trento
Fondazione Bruno Kessler – FBK
Borse di studio/ Scholarships

E	**Modeling to investigate emerging and re-emerging infectious diseases**

Topic: Mathematical and computational modeling to investigate emerging and re-emerging infectious diseases

P.I.: PUGLIESE ANDREA (Unitn) – POLETTI PIERO (Fbk)

Contacts: andrea.pugliese@unitn.it – poletti@fbk.eu

Synthetic description of the activity and expected research outcome

Research activities conducted during the Ph.D. program will focus on mathematical and statistical modeling aimed at investigating the transmission of emerging and re-emerging infectious diseases within human populations. These may include the development and analysis of epidemiological models for disease spread, the integration and analysis of diverse data sources, the application of Bayesian statistical inference to epidemiological records, as well as the development of novel computational approaches to simulate epidemic trajectories and evaluate the impact of public health interventions on disease transmission.

References

[1] A Zardini, F Menegale, A Gobbi, M Manica, G Guzzetta, V d'Andrea, et al. (2024). Estimating the potential risk of transmission of arboviruses in the Americas and Europe: a modelling study. The Lancet Planetary Health 8 (1), e30-e40

[2] CM Grané, P Mancuso, M Vicentini, F Venturelli, O Djuric, M Manica, et al. (2023). SARS-CoV-2 transmission patterns in educational settings during the Alpha wave in Reggio-Emilia, Italy. Epidemics 44, 100712

[4] HJ Ang, F Menegale, G Preziosi, E Pariani, M Migliari, L Pellegrinelli, et al. (2023). Reconstructing the impact of COVID-19 on the immunity gap and transmission of respiratory syncytial virus in Lombardy, Italy. EBioMedicine 95

[4] V Marziano, G Guzzetta, BM Rondinone, F Boccuni, F Riccardo, A Bella, et al. (2021). Retrospective analysis of the Italian exit strategy from COVID-19 lockdown. Proc Natl Acad Sci U S A. 118(4):e2019617118. doi: 10.1073/pnas.2019617118.

[5] Marini, G., Calzolari, M., Angelini, P., Bellini, R., Bellini, S., Bolzoni, L., Torri, D., Defilippo, F., Dorigatti, I., Nikolay, B., Pugliese, A., Rosà, R., Tamba, M., (2020). A quantitative comparison of West Nile virus incidence from 2013 to 2018 in Emilia-Romagna, Italy. PLoS Negl. Trop. Dis. 14, e0007953. Doi: 10.1371/journal.pntd.0007953

Ideal candidate

Ideal candidates will have a degree in applied mathematics or related areas, some experience in mathematical modelling, and a good competence of scientific programming; knowledge of basic statistical methods would be a plus.