SHORT BIOS

1) My name is Vojtech Suchanek, and I am a Ph.D. student at the Center of Cryptography Research and Security (CRoCS). I did both bachelor's and master's degrees in Mathematics at MU. My bachelor's thesis focused on permutation groups in number theory. I continued my focus on number theory in my master's thesis, which was done at the Faculty of Informatics. The thesis topic was isogeny volcanoes in cryptography, where I studied modern isogeny-based protocols and their usage in post-quantum cryptography. After graduating, I joined the CROCS team as one of the experts in mathematical cryptography. I am currently working on the analysis of isogenies of standardized elliptic curves and general algorithms relating to the RSA cryptosystem.

2) Lukáš Sadlek is currently pursuing a Ph.D. degree in computing technology and methodology with the Faculty of Informatics, Masaryk University, where he is a researcher with the Institute of Computer Science and a member of the University's Security Team (CSIRT-MU). Since 2017, he has cooperated with CSIRT-MU on a research project as a junior cybersecurity researcher and developer where he was responsible for the design and development of tools for cyber situational awareness and decision support in the protection of critical infrastructures. During his Ph.D. study, he attempts to improve security operations management using his experiences with programming theory, modern technologies, theoretical computer science and statistics gained during previous studies. His research interests also include cyber situational awareness and vulnerability management.

3) My name is Miriama Jánošová. I am a PhD candidate at the Laboratory of Data Intensive Systems and Applications (DISA), Faculty of Informatics, Masaryk University, Brno. I joined my current team during my Master's Degree studies. At that time, I focused on creating algorithms for the selection of representatives of multidimensional

data clusters. The analysis of unstructured data has remained the focal point of my efforts during my PhD studies. At the moment, I am dedicated to the cluster analysis of the motion capture data. My goal is to propose new approaches to Similarity-based Data Analytics that would lower the computational demands.

4) My name is Jan Jancar and I am a PhD candidate at the Centre for Research on Cryptography and Security (CRoCS) at Masaryk University, Czech Republic. My previous work at CRoCS has focused on elliptic curve cryptography (ECC) and security of programmable smartcards. This research resulted in the discovery of several real-world vulnerabilities, of which the most impactful was the Minerva vulnerability, which is? a group of side-channel vulnerabilities in implementations of the ECDSA cryptosystem. Currently, I am working in the field of constant-time cryptography and side-channels.

5) My name is Antonín Dufka, and I am a Ph.D. student at the Centre for Research on Cryptography and Security (CRoCS). I obtained a bachelor's and a master's degree in computer science with a focus on information security at Masaryk University. In my master's thesis, I worked on multi-party computation using Schnorr signatures with smartcards in the context of Bitcoin. The experience from this work evolved into my interest in the area of secure multi-party computation. My current research focuses on secure multi-party protocols executed by secure but resource-constrained devices like smartcards, smartphones, and hardware cryptocurrency wallets.

6) My name is Michal Ajdarów, and I am a PhD candidate at the department of computer science of Masaryk University. During my Master's Degree studies, I began working on the area of various stochastic systems with energy constraints. My master's thesis focused on the Partially-observable Markov decision processes with consumption objectives in particular. I continued with this area for my PhD studies. Currently, I am focusing on designing new algorithms for determining the termination complexity of Vector addition systems

with states. Other areas of interest also include game theory and probability theory.

7) Filip Opálený is a Ph.D. student with research interests in molecular visualizations. Affiliated with Visitlab, the Department of Visual Computing, Faculty of Informatics, MUNI, Brno, he is collaborating on various projects with multiple research teams at the Faculty of Science, MUNI, Brno. His current projects include developing a visual tool for the rational design of aperiodic structures in proteins, researching novel visualisation methods for the exploration of genomic data and chromatin structures.

8) Krištof Anetta is an interdisciplinary researcher at the Natural Language Processing Centre, Faculty of Informatics, Masaryk University. His current research focuses on knowledge extraction from electronic health records.
His qualifications include a master's degree in Cognitive Science (MEi:CogSci at the University of Vienna), a master's degree in English Language and Literature (Masaryk University), and a bachelor's degree in Psychology (Comenius University in Bratislava). Before becoming a researcher, he spent several years working as a programmer for international companies, acquainting himself with a rich assortment of technologies and frameworks.
Outside of computer science, literature and writing constitute his major fields of interest and engagement. He is an occasional translator and teaches college-level literature and history courses