# Researcher from FIIT STU discovered a way to reveal a developer´s intellectual property from a microchip.

*Bratislava 19 October 2021*

*Press release*

**Neural networks are one of the basic building blocks of artificial intelligence. Their model and internal parameters are heavily protected by authors as a trade secret, which serves as their competitive advantage. In her latest publication, researcher Dr. Xiaolu Hou, who came to the Faculty of Informatics and Information Technology STU (FIIT STU) from Singapore, how the whole neural network model can be extracted and revealed from a microchip.**

"*Our research has shown that neural networks are vulnerable to error- causing attacks. These attacks change the physical behavior of the device during calculation, resulting in a change of the calculated value. Previous work has mostly examined attacks on bugs due to incorrect output classification, which affected the reliability of neutral networks. We explored the possibilities of reverse engineering neural networks with error attacks,*" explain researchers around Dr. Xiaolu Hou from FIIT STU.

Article with their findings was published in the prestigious peer-reviewed journal IEEE Transactions on Reliability, which belongs to the highest category Q1 in computer science with a high citation rate.

"*In this research, we have developed a method that provides demonstrably accurate extraction of neural network parameters by inserting errors. The goal of our method is to restore specific layers of the neutral networks, which allows us to see its key parameters and thus reveal what developers consider to be their intellectual property*," says Dr. Xiaolu Hou.

"Cyber security is an extremely important issue that some of our colleagues have been working on for decades. In recent years, the importance of computer security has grown even more dynamically than in the past, and much more directly affects each of us. It is great to see that the arrival of new colleagues from abroad to our faculty reflects in the form of such high-quality scientific publications, which are unquestionably at the top worldwide level," says prof. Ivan Kotuliak, Dean of FIIT STU.

Dr. Xiaolu Hou currently works as an assistant professor at the Faculty of Information and Information Technology of the Slovak University of technology in Bratislava. In 2017, she received a doctorate in mathematics from Nanyang Technological University (NTU) in Singapore. Her research is focused on hardware security of cryptography and neural networks. She is also experienced in research of location privacy, multiparty computation, and differential privacy. Thanks to a wide range of research interests, she presented her works at the most prestigious conferences and in journals in various fields, from mathematics to computer security. She started working at FIIT STU at the beginning of 2021, along multiple other experts from abroad who recently came to the faculty. Today, in addition to active research at the faculty, she also works as a lecturer and conducts student´s diploma theses.