January 22, 2025

Department of Homeland Security
United States Citizenship and Immigration Services

Re: Independent Letter of Support for Dr. Kirill Nikitin

Dear USCIS Officer,

I am providing this independent letter to confirm that Dr. Nikitin is an outstanding researcher, and I enthusiastically support the petition to classify him as a scientist of extraordinary ability based on his impressive scientific contributions and his reputation as a leader in the field.

I am …

Although I have not worked directly with Dr. Nikitin, I offered him a position as a postdoctoral researcher in my group in 2021, which has allowed me to become well-acquainted with his work and accomplishments. Dr. Nikitin has made significant, original contributions to the field of data and computer privacy, particularly through his research on Private Information Retrieval (PIR). PIR enables users to retrieve data from a computer database without revealing what data they are accessing. This technology is crucial for improving the privacy guarantees of online communication, for example, in instant messaging applications, such as WhatsApp. Previously, research in PIR assumed that database servers always followed the protocol perfectly. In real-world applications, however, a corrupted or compromised server can violate the protocol and attempt to break the user's privacy. Dr. Nikitin has demonstrated that such a server can alter its response to a user's query, observe whether the user accepts this response, and, subsequently, infer what data have been accessed. Dr. Nikitin's proposed schemes are the first efficient solution to ensure the privacy of information retrieval even when the database server is malicious. This achievement bridges the gap between theoretical PIR protocols and their practical security in real-world scenarios.

Dr. Nikitin has also advanced blockchain research by demonstrating how to integrate state-of-the-art verifiable outsourced computation into permissioned or permissionless blockchains. In essence, a blockchain achieves strong integrity protection through the redundant verification of all blocks and the transactions they contain by numerous—e.g., thousands or tens of thousands—of independent decentralized participants. The key idea of Piperine, the system that Dr. Nikitin and his collaborators from Microsoft

Research designed, is to reduce this large redundant verification cost by allowing a single untrusted prover to produce a verifiable cryptographic proof of the correctness of a block of transactions and the many independent verifiers to merely verify these proofs, instead of the transactions themselves. While simple in concept, the key technical challenges are in bridging the huge remaining efficiency gap between state-of-the-art outsourced computation and direct re-execution, as well as the many limitations and impedance mismatches between current outsourced computation methods and the requirements of the blockchain context. I believe that Piperine represents a major contribution both to blockchain and outsourced computation research, and it illustrates Dr. Nikitin's breadth and independent collaboration abilities in security/privacy research.

Another evidence of Dr. Nikitin's recognition as a leading expert in the field is his role in judging the work of other researchers. He has already served on the Program Committee for such prestigious conferences in computer security and privacy as the ACM Conference on Computer and Communications Security, the USENIX Security Symposium, and the IEEE International Conference on Blockchain and Cryptocurrency. Invitations to join the Program Committee of such conferences are extended only to internationally renowned scientists, as the members do not only provide their experts reviews but also participate in the discussion and make collective final decisions of either accepting or rejecting submissions. I can confirm that Dr. Nikitin possesses the highest level of expertise required for this role, as both he and I were active Program Committee members of the ACM Conference on Computer and Communications Security. His contributions underscore his deep understanding of complex technical concepts and his ability to evaluate their significance and potential impact. Finally, his active participation demonstrates not only his professional standing among peers but also his dedication to advancing the field of computer security and privacy.

In conclusion, Dr. Nikitin is recognized internationally for his research contributions and his service to the research community. His abilities and knowledge are an important asset to the economy and scientific standing of the United States. I strongly support his petition for classification as a scientist of extraordinary ability.

Sincerely yours,

CCC