February 27, 2025

United States Citizenship and Immigration Services

Re: Independent Supporting Letter for the Immigration Petition of Dr. Kirill Nikitin

Dear Sir/Madam,

I write this letter in my capacity as … to offer my strong endorsement of Dr. Kirill Nikitin's immigration petition. Although I have never worked with Dr. Nikitin, I have followed his research with great interest. As a distinguished researcher in computer privacy and security, Dr. Nikitin has conducted innovative work that has significantly advanced both the theoretical and practical aspects of the field. His exceptional contributions clearly demonstrate his extraordinary abilities and promise considerable benefits to the global community.

I would like to begin by introducing myself. My name is …

My research work examines …

Dr. Nikitin is foremost known for his scientific contributions in data privacy and, specifically, in the area of metadata protection. In his paper titled "Reducing metadata leakage from encrypted files and communication with PURBs" published in the Proceedings on Privacy Enhancing Technologies, Dr. Nikitin presented techniques for both obfuscating the length of encrypted content and protecting encryption metadata. The length can reveal a significant amount of information about content but protecting it is a non-trivial task because digital objects can radically differ in size. A user might send a short email or download a large movie in the same Web session and making the two the same size is impractical—the Internet does not have enough bandwidth to handle emails that are gigabytes in size. Dr. Nikitin came up with padding technique that accounts for the size of an object and adds just enough protection bytes to provide provable privacy guarantees while still ensuring practicality. The technique is one of the kind and has already been adopted by some major technological companies.

The techniques for protecting encryption metadata by Dr. Nikitin were the first to provide scalable encryption functionality for ciphertexts (encrypted data) with hundreds of recipients. Part of my research is on anonymity networks where users can communicate with each other without revealing their communication patterns. These networks require that ciphertexts do not expose the identities of their recipients, but prior protection approaches for this scaled to only several recipients. The fact that Dr. Nikitin's techniques overcome this barrier and further extend the protection to other types of encryption metadata is a major achievement for the field.

Dr. Nikitin has also made notable advance in blockchain research. In his paper titled "Replicated state machines without replicated execution", he demonstrates that the throughput of blockchains networks can be increased by using verifiable computation. Specifically, if, instead of sending out multiple transactions, a blockchain node proves the correctness of their cumulative execution and sends out this proof, other nodes can verify the proof faster than they would have re-executed the transactions. This was a surprising result that showcased Dr. Nikitin's expertise on the topic and his ability to design innovative solutions. Furthermore, in his other paper titled "Chainiac: Proactive software-update transparency via collectively signed skipchains and verified builds", he introduced a novel data structure named skipchain. Unlike traditional blockchains, a skipchain facilitates verifiable forward traversal of the blocks and more efficient backward traversal. This is another example of an innovative creation that makes Dr. Nikitin is a leading researcher in the field.

It comes as no surprise that the work by Dr. Nikitin is widely published and cited by researchers worldwide. He has publications in premier computer security and privacy venues, such as the USENIX Security Symposium and the IEEE Symposium on Security and Privacy. His work has already attained over 300 citations from his peers, attesting to its significant influence on the field. This impressive for his career stage citation count underscores the far-reaching impact of his research, which not only enriches academic discourse but also drives the development of real-world solutions in data privacy and security. Such widespread recognition is a clear indicator of Dr. Nikitin's exceptional contributions and reinforces his eligibility as an individual of extraordinary ability.

In summary, I offer my unequivocal support for Dr Kirill Nikitin's immigration petition. His pioneering research and outstanding contributions to computer privacy and security not only advance our understanding of critical challenges in the field, but also facilitate the development of innovative solutions. I am confident that his work will continue to have a significant impact on both academic research and technological practice, and I trust that his application will be granted the favourable consideration it richly deserves. Should you require any further information, please do not hesitate to contact me.

Yours faithfully,

EEE