

January 25, 2018

## Letter of Support for the Grant Proposal by Bogdan Warinschi

To whom it may concern,

I have been recently awarded a grant by the US National Science Foundation (NSF award #1749069) for the project “SaTC: EAGER: Collaborative: Quantifying Information Leakage in Searchable Encryption”. This highly collaborative interdisciplinary project aims to clarify our understanding of the leakage associated with various searchable encryption schemes and to achieve quantitative assessments of the risks to confidentiality by merging the perspectives of the areas of quantitative information flow and provable security. The co-PIs are myself and Professor Geoffrey Smith from the Florida International University. We are the experts in provable security and quantitative information flow respectively.

I would like to confirm that the ideas underlying the award came from a joint research meeting I, Geoffrey Smith and Bogdan Warinschi had previously held. In fact, Bogdan had initially connected me and Geoffrey Smith for the purpose of joint work.

Accordingly, it will be extremely useful for the progress of our research if Bogdan Warinchi could visit the US for some time, probably for 3 10-day visits. It is much more productive to collaborate in person than remotely. I would like to host Bogdan at Georgia Tech, where he can get an office. But my grant is not sufficient to provide financial support.

Please contact me in case of any questions.

Sincerely,



Alexandra Boldyreva  
Associate Professor  
School of Computer Science  
College of Computing  
Georgia Institute of Technology  
sasha@gatech.edu