Revised 05/01/2020 **NSF BIOGRAPHICAL SKETCH** **OMB-3145-0058**

NAME: Ni Trieu

POSITION TITLE & INSTITUTION: Assistant Professor, Arizona State University, Tempe, AZ

A. PROFESSIONAL PREPARATION
(see PAPPG Chapter II.C.2.f.(i)(a))

INSTITUTION	LOCATION	MAJOR/AREA OF STUDY	DEGREE (if applicable)	YEAR (YYYY)
St. Petersburg State Polytechnic University	Petersburg, Russia	Computer Science	B.Sc.	2013
Oregon State University	Corvallis, OR	Computer Science	M.S	2017
Oregon State University	Corvallis, OR	Computer Science	Ph.D	2020

B. APPOINTMENTS
(see PAPPG Chapter II.C.2.f.(i)(b))

From - To	Position Title, Organization and Location
Aug/2020 - Present	Assistant Professor, Arizona State University, AZ
Mar/2020 - Aug/2020	Postdoctoral researcher, UC Berkeley, CA
Jun/2019 - Sept/2019	Research Intern, Google, NY
Jun/2018 - Sept/2018	Research Intern, Visa Research, CA
Jun/2017 - Aug/2017	Research Intern, Bell Labs, NJ
Jun/2016 - Aug/2016	Research Intern, Bell Labs, NJ
Sept/2014- Sept/2015-	Research Assistant, Singapore University of Technology and Design, Singapore

C. PRODUCTS

(see PAPPG Chapter II.C.2.f.(i)(c))

Products Most Closely Related to the Proposed Project

1) G. Garimella, B. Pinkas, M. Rosulek, N. Trieu, and A. Yanai, "Oblivious Key-Value Stores and Amplification for Private Set Intersection" in the 41th International Cryptology Conference (CRYPTO), 2021.

2) M Rosulek, N. Trieu "Compact and Malicious Private Set Intersection for Small Sets" In 28th ACM Conference on Computer and Communications Security (CCS), 2021

3) T. Duong, D. H. Phan, N. Trieu, "Catalic: Delegated PSI Cardinality with Applications to Contact Tracing", in the 26h Annual International Conference on the Theory and Application of Cryptology and Information Security (Asiacrypt), 2020

4) B. Pinkas, M. Rosulek, N. Trieu, and A. Yanai, "PSI from PaXoS: Fast, Malicious Private Set Intersection", in the 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT), 2020.

5) P. Mohassel, M. Rosulek, and N. Trieu, "Practical Privacy-Preserving K-means Clustering", in the 20th Privacy Enhancing Technologies Symposium (PETs), 2020

Other Significant Products, Whether or Not Related to the Proposed Project

1) O. Nevo, N. Trieu, A. Yana "Simple, Fast Malicious Multiparty Private Set Intersection" In 28th ACM Conference on Computer and Communications Security (CCS), 2021
2) B. Pinkas, M. Rosulek, N. Trieu, and A. Yanai, "SpOT-Light: Lightweight Private Set Intersection from Sparse OT Extension", in the 39th International Cryptology Conference (CRYPTO), 2019.
3) V. Kolesnikov, M. Rosulek, N. Trieu, and X. Wang, "Scalable Private Set Union from Symmetric-Key Techniques", in the 25th (Asiacrypt), 2019.
4) D. Demmler, P. Rindal, M. Rosulek, and N. Trieu, 'PIR-PSI: Scaling Private Contact Discovery", in the 18th Privacy Enhancing Technologies Symposium (PETS), 2018.
5) C. Hauser, S. Nilizadeh, Y. Shoshitaishvili, G. Vigna, C. Kruegel, N. Trieu, S. Ravi, "Street Rep: A Privacy-Preserving Reputation Aggregation System", in submission

D. SYNERGISTIC ACTIVITIES

(see PAPPG Chapter II.C.2.f.(i)(d))

1) Conference Program Committee for 2021 Crypto and Security conferences: 41th International Cryptology Conference (CRYPTO), 2021.
2) Active reviewer for 2018–2021 ML, Crypto, and Security conferences/journals: the 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT), 2021
3) Invited speaker at the Microsoft Research Cryptography Colloquium (Aug/2020)
4) Faculty Search Committee: Arizona State University, 2021
5) NSF SaTC Panel Reviewer (2020)
6) Teaching CSE 598 (Special Topics: Secure Computation for Machine Learning) in Spring 2021.