Nguyen Phuong Ha

Contact Information

Department of Electrical and Computer Engineering,
University of Connecticut,
Storrs,
CT 06269-4157, United States.

phuongha.ntu@gmail.com

Citizenship

Vietnamese, US Greencard in the category National Interest Waiver (E21).

Research Interests

My research focuses on the following important related topics: Machine Learning and Information Security.

Machine Learning. Conducted research on Large Scale Optimization, Artificial Intelligence, Security and Privacy in Machine Learning.

- **Large Scale Optimization**. Worked on fundamental problems such as the convergence of Stochastic Gradient Descent (SGD) and Asynchronous Stochastic Gradient Descent (Hogwild!) (Distributed Machine Learning), the structure of Deep Neural Networks.
- **Artificial Intelligence**. Studied fundamental problems of Deep Learning and Reinforcement Learning, i.e., focus on the efficiency and enhancement of Deep Learning and Reinforcement Learning.
- **Security and Privacy in Machine Learning**. Studied fundamental problems such as Adversarial Machine Learning and Differential Privacy Machine Learning.

Information Security. Conducted research on Cryptography, Side Channel Analysis and Hardware Security.

- **Cryptography**. Cryptanalysed the symmetric key ciphers such as block ciphers SERPENT, KASUMI, and stream cipher ZUC and improved the cryptanalytic tool Multidimensional Linear Cryptanalysis.
- **Side Channel Analysis**. Worked on Cache Attack, Power Analysis and Threshold Implementations Countermeasure. Improved the Masking countermeasure used in SCA.
- **Physically Unclonable Functions (PUF)**. Published on the security of some PUF designs under cryptanalysis, machine learning based modeling attacks and side channel attacks. Introduced the first machine learning resistant lightweight strong PUF design.

Awards and Scholarships

- Red Diploma (1st class honor) 2008
- Scholarship of Vietnam government for studying in Russia 2003-2008
- Scholarship of Singapore International Graduate Award (SINGA) for PhD program in Singapore 2008-2012

Research Group

- Co-organizer of Multi-university Research Group on Security and Privacy in Machine Learning , USA-VietNam 2019
- Co-organizer of Security Seminar at University of Connecticut, USA 2017-2018

Industry Activity

- Member in Advisor Board for security and artificial intelligence at Autonomous Inc (`https://www.autonomous.ai/`), New York City, USA. 2019

Research Activity

Conferences and Workshop

- Serve as a member in program committee at ASHES, England 2019
- Serve as a member in program committee at ASHES, Canada 2018
- Serve as a member in program committee at SPACE, India 2015
- Given an tutorial at IEEE VLSID, India 2015
- Give an invited talk at VDAT, India 2014
- Serve as a session chair at VDAT, India 2014
- Serve as a member in program committee at INDOCRYPT, India 2014
- Give an invited tutorial at SPACE, India 2014

Education

Nanyang Technological University, Singapore

Doctor of Philosophy, School of Physical and Mathematical Sciences, 2008-2013

- Thesis Topic: *On Design and Analysis of Symmetric Key Ciphers*
- Advisors: Professor Wang Huaxiong

Moscow State University Lomonosov, Moscow, Russia

Specialist of Applied Mathematics and Informatics, Faculty of Computational Mathematics and Cybernetics, 2003-2008

- Thesis Topic: *Studying and Implementing cryptosystem PGM on* $GF(2)^n$
- Advisors: Professor Eduard Andreevich Primenko

Research Experience

Research Fellow March 2016 to now
Department of Electrical and Computer Engineering,
University of Connecticut, Storrs, United States.
Supervisor: Prof Marten Van Dijk

Research Fellow February 2014 to December 2015
Department of Computer Science and Engineering,
Indian Institute of Kharagpur, WB, India.
Supervisor: Prof Debdeep Mukhopadhyay

Research Associate August 2012 to August 2013
Temasek Lab@ NTU,
Nanyang Technological University
Supervisor: Prof Axel Poschmann

Research Publications

1. **Phuong Ha Nguyen**, Lam M. Nguyen, Marten van Dijk: Tight Dimension Independent Lower Bound on Optimal Expected Convergence Rate for Diminishing Step Sizes in SGD. (NeurIPS) 2019.

2. Lam M. Nguyen*, **Phuong Ha Nguyen***, Peter Richtrik, Katya Scheinberg, Martin Takc, Marten van Dijk: New Convergence Aspects of Stochastic Gradient Algorithms. Accepted with minor revision at Journal of Machine Learning Research (JMRL) 2019. * equal contribution.

3. **Phuong Ha Nguyen**, Durga Prasad Sahoo, Chenglu Jin, Kaleel Mahmood, Ulrich Rhrmair, Marten van Dijk: (Long Paper) The Interpose PUF: Secure PUF Design against State-of-the-art Machine Learning Attacks. Transactions of Conference on Cryptographic Hardware and Embedded Systems (TCHES) 2019. Github: `https://github.com/scluconn/DA_PUF_Library`

4. Marten van Dijk, Lam M. Nguyen, **Phuong Ha Nguyen**, Dzung T. Phan: Characterization of Convex Objective Functions and Optimal Expected Convergence Rates for SGD. International Conference on Machine Learning (ICML) 2019.

5. Raihan Sayeed Khan, Nafisa Noor, Chenglu Jin, Sadid Muneer, Faruk Dirisaglik, Adam Cywar, **Phuong Ha Nguyen**, Marten van Dijk, Ali Gokirmak, Helena Silva: Exploiting Lithography Limits for Hardware Security Applications. IEEE International Conference on Nanotechnology (IEEE NANO) 2019. (Best paper award candidate)

6. Lam M. Nguyen, **Phuong Ha Nguyen**, Marten van Dijk, Peter Richtrik, Katya Scheinberg, Martin Takc: SGD and Hogwild! Convergence Without the Bounded Gradients Assumption. International Conference on Machine Learning (ICML) 2018.

7. Durga Prasad Sahoo, Debdeep Mukhopadhyay, Rajat Subhra Chakraborty, **Phuong Ha Nguyen**: A Multiplexer based Arbiter PUF Composition with Enhanced Reliability and Security. IEEE Transactions on Computers (TC) 2018.

8. **Phuong Ha Nguyen**, Durga Prasad Sahoo, Rajat Subhra Chakraborty and Debdeep Mukhopadhyay: Security Analysis of Arbiter PUF and Its Lightweight Compositions Under Predictability Test. IEEE Transactions on Design Automation of Electronic Systems (TODES) 2017.

9. Durga Prasad Sahoo, **Phuong Ha Nguyen**, Debapriya Basu Roy, Debdeep Mukhopadhyay, Rajat Subhra Chakraborty: Side Channel Evaluation of PUF-Based Pseudorandom Permutation. DSD 2017.

10. **Phuong Ha Nguyen**, Durga Prasad Sahoo, Rajat Subhra Chakraborty, Debdeep Mukhopadhyay: Efficient Attacks on Robust Ring Oscillator PUF with Enhanced Challenge-Response Set. DATE 2015.

11. Debdeep Mukhopadhyay, Rajat Subhra Chakraborty, **Phuong Ha Nguyen**, Durga Prasad Sahoo: Physcially Unclonable Functions: A Promising Security Primitive for Internet of Things (Long tutorial). VLSID 2015.

12. Sikhar Patranabis, Abhishek Chakraborty, **Phuong Ha Nguyen** and Debdeep Mukhopadhyay: Physcially Unclonable Functions: A Biased Fault Attack on the Time Redundancy Countermeasure for AES. COSADE 2015.

13. Durga Prasad Sahoo, **Phuong Ha Nguyen**, Debdeep Mukhopadhyay and Rajat Subhra Chakraborty: A Case of Lightweight PUF Constructions: Cryptanalysis and Machine Learning Attacks. Accepted in IEEE TCAD 2015.

14. Sebastian Kutzner, **Phuong Ha Nguyen**, Axel Poschmann, Marc Stottinger: Minimizing S-Boxes in Hardware by Utilizing Linear Transformations. AFRICACRYPT 2014.

15. **Phuong Ha Nguyen**, Durga Prasad Sahoo, Debdeep Mukhopadhyay, Rajat Subhra Chakraborty: Cryptanalysis of Composite PUFs (Invited Talk). VDAT 2014.

16. **Phuong Ha Nguyen**, Durga Prasad Sahoo: Lightweight and Secure PUFs: A Survey (Invited Paper). SPACE 2014.

17. Sebastian Thomas Kutzner, **Phuong Ha Nguyen**, Axel Poschmann and Huaxiong Wang: On 3-share Threshold Implementations for 4-bit S-boxes . COSADE2013.

18. Sebastian Thomas Kutzner, **Phuong Ha Nguyen**, Axel Poschmann: Enabling 3-share Threshold Implementations to any 4-bit S-boxes . ICISC2013.

19. Chester Rebeiro, **Phuong Ha Nguyen**, Debdeep Mukhopadhyay and Axel Poschmann: Formalizing the Effect of Feistel Cipher Structures on Differential Cache Attacks. IEEE Transactions on Information Forensics and Security journal 2013.

20. **Phuong Ha Nguyen**, Chester Rebeiro, Debdeep Mukhopadhyay and Huaxiong Wang: Improved Differential Cache-Trace Attacks on SMS4. INSCRYPT2012.
21. Hongjun Wu, Tao Huang, **Phuong Ha Nguyen**, Huaxiong Wang, and San Ling: Differential Attacks against Stream Cipher ZUC. ASIACRYPT2012.
22. **Phuong Ha Nguyen**, Hongjun Wu, Huaxiong Wang: Improving the Algorithm 2 in Multidimensional Linear Cryptanalysis. ACISP 2011.
23. **Phuong Ha Nguyen**, Matthew J. B. Robshaw, Huaxiong Wang: On Related-Key Attacks and KASUMI: The Case of A5/3. INDOCRYPT 2011.
24. **Phuong Ha Nguyen**, Lei Wei, Huaxiong Wang, San Ling: On Multidimensional Linear Cryptanalysis. ACISP 2010.

Book Chapter

1. Raihan Sayeed Khan, Nafisa Noor, Chenglu Jin, Jake Scoggin, Zachary Woods, Sadid Muneer, Aaron Ciardullo, **Phuong Ha Nguyen**, Ali Gokirmak, Marten van Dijk, and Helena Silva. Chapter 6: Phase Change Memory and its Applications in Hardware Security in book Security Opportunities in Nano Devices and Emerging Technologies, Publisher: CRC Press, pp.93-114, 2017.

Unpublished Works or Works In Submission

1. Lam M. Nguyen, Marten van Dijk, Dzung T. Phan, **Phuong Ha Nguyen**, Tsui-Wei Weng, Jayant R. Kalagnanam: Optimal Finite-Sum Smooth Non-Convex Optimization with SARAH. CoRR abs/1901.07648 (2019)
2. **Phuong Ha Nguyen** and Durga Prasad Sahoo: An Efficient and Scalable Modeling Attack on Lightweight Secure Physically Unclonable Function. See http://eprint.iacr.org/2016/428.pdf
3. Durga Prasad Sahoo, **Phuong Ha Nguyen**, Rajat Subhra Chakraborty and Debdeep Mukhopadhyay: Architectural Bias: a Novel Statistical Metric to Evaluate Arbiter PUF Variants. See http://eprint.iacr.org/2016/057.pdf

Computer Programming

- Matlab, Python, TensorFlow and Keras
- Library for Machine Learning Analysis on Interpose PUF
  https://github.com/scluconn/DA_PUF_Library

Reviewer

- ASHES2019
- ASHES2018
- IEEE-TDSC2018
- GLSVLSI2017
- HOST2017
- DAC2017
- ACISP2017
- IEEE-TC2017
- ASHES2017
- IEEE-TDSC2017
- IEEE-TETC2016
- COSADE2015
- SPACE2015
- CHES2015
- IEEE-TCAD2014
- ICISS2014

- INDOCRYPT2014
- ACISP2013
- COSADE2013
- IWSEC2013
- RFIDsec2013
- ICICS2012
- IWSEC2012
- AISC2012
- FSE2011
- SKEW2011

Presentations

Conferences and Workshop

- NeurIPs, Canada 2019
- CHES, USA 2019
- ICML, USA 2019
- DIMAC/MOPTA, USA 2018
- DATE, France 2015
- VLSID, India 2015
- VDAT, India 2014
- SPACE, India 2014
- COSADE, France 2013
- WAS, Singapore 2013
- INSCRYPT, China 2012
- ACISP, Australia 2011
- INDOSCRYPT, India 2011

Teaching Experience

Teaching Assistant — Summer 2017
Hardware Security
Electrical and Computer Engineering,
University of Connecticut

Teaching Assistant — Summer 2011
Calculus I
School of Physical and Mathematical Sciences,
Nanyang Technological University

Teaching Assistant — Summer 2010
Calculus I
School of Physical and Mathematical Sciences,
Nanyang Technological University