Duc Tri Nguyen

- Pragmatic High-speed Cryptographic Engineering
- 4 times Olympiad in Cryptography Winner
- Proven track records in Security Competition

Github
Profile
Google Scholar
dnguye69@gmu.edu

Education

George Mason University *2017.09 - Present*
Fairfax, VA, USA

Ph.D. in Computer Engineering
Advised by Kris Gaj

- High-speed PQC Hardware Cryptographic Engineering
- ARMv8 NEON Acclerated Post-Quantum Cryptography Finalists
- SUPERCOP Contributor: SABER, NTRU, CRYSTALS-Kyber
- DAGS Post-Quantum Cryptography Submission Team

HCMUT University of Technology *2010.09 - 2015.11*
Ho Chi Minh, Vietnam

🎓 **B.S. in Computer Engineering**
Computer Science and Engineering

Publication

HLS in Implementing and Benchmarking NTT in Lattice-based PQC using SW/HW Codesign
**Duc Tri Nguyen, Viet B. Dang, and Kris Gaj*, Applied Reconfigurable Computing (ARC 2020)

A HLS Approach to the SW/HW Codesign of NTT-based Post-Quantum Cryptography Algorithms
**Duc Tri Nguyen, Viet B. Dang, Kris Gaj*, Field-Programmable Technology (FPT 2019)

SW/HW Codesign of the PQC Algorithm NTRUEncrypt Using HLS and RTL Design Methodologies
*Farnoud Farahmand, *Duc Tri Nguyen, Viet B. Dang, Ahmed Ferozpuri, Kris Gaj*,
Field Programmable Logic and Applications (FPL 2019)

DAGS: Reloaded Revisiting Dyadic Key Encapsulation
Gustavo Banegas et al., Code-Based Cryptography 2019 (CBC 2019)

Evaluating the Potential for Hardware Acceleration of Four NTRU-Based Key Encapsulation Mechanisms Using SW/HW Codesign
*Farnoud Farahmand, Viet B. Dang, *Duc Tri Nguyen, Kris Gaj*,
Post-Quantum Cryptography (PQC 2019)

Experiences

GE Global Research 2021.05 - 2021.08

Controls & Optimization Technology Domain
Research Intern

VNG Corporation 2014.12 - 2015.04

Operation Security Internship
Incident Response Intern

Technologies

Experienced	`Hardware Design, Cryptography, Reverse Engineering`
Low-level	`ARMv8, NEON, x86_64, AVX2`
High-level	`Python, C/C++, Bash, Verilog, VHDL, Tcl`
Tools	**`IDA, Ghidra, Z3Prover, Radare2`**
Hardware	`FPGA:` **`Xilinx Vitis`** `| GPU: OpenACC`
Libraries	`Z3Prover, SageMath, Pwntools`

Honors & Awards

International Students' Olympiad in Cryptography

NSUCrypto Professional Round 2019 **3rd**
December 2nd 2019

NSUCrypto Professional Round 2018
December 3rd 2018

NSUCrypto Professional Round 2017 **3rd**
December 21st 2017

NSUCrypto Professional Round 2016 **3rd**
An answer to one of the problems nominated as a best solution
December 14th 2016

Mid-Atlantic Collegiate Cyber Defense Competition

MACCDC 2021 Regional Final Round **2nd**
1st place in Services, April 2021__

MACCDC 2021 Regional Qual Round **1st**
1st place in Services, February 2021__

MACCDC 2020 Regional Final Round 5th
Tied 1st place in Services, April 2020

MACCDC 2020 Regional Qual Round *1st place in Services, March 2020*	

Capture The Flag

MetaCTF 2020 University of Viginia, VA, USA	**2nd** / Debugmen
PatriotCTF 2020 George Mason University, VA, USA	**3rd** / Efiens
UMDCTF 2020 University of Viginia, VA, USA	4th / MasonCC
MetaCTF University of Viginia, VA, USA	**1st** / BackToBack
Pros Vs Joes 2019 BSides DC, Washington DC, USA	**2nd** / Honk_Honk_Honk
VTSummit 2019 Virginia Tech - VA, USA	**1st** / MasonCC
UMBC Cyber Dawgs 2019 University of Maryland - MD, USA	**2nd** / MasonCC
2016 CTF Worldwide Team Ranking *1st in the world*	**1st / DCUA**
CSAW Finalist 2016 NYU Abu Dhabi, United Arab Emirates	**1st** / DCUA
ASIS Final Round 2016 Iran Cyber Security Contest	**1st** / DCUA
Hack in the Box Singapore 2016 Facebook, Singapore	4th / DCUA
HITB CTF Amsterdam 2015 Amsterdam, The Netherlands	**2nd** / DCUA
National Cyber Security 2014 VNISA, Vietnam	**2nd** / BKIT-Respawn

Qualifications

International Students' Olympiad in Cryptography 2016-2019	Novosibirsk State University
Lattices and Applications to Cryptography 2016	CIMPA
Cryptography: Foundations and New Directions 2016	IACR-SEAMS School
ECSI Hacker Playground 2015	National Hero Certificate

Services

I am founder of Efiens Security club. Efiens club is where computer security enthusiasts unified, we focus on modern security topic in many areas such as *Cryptography, Binary Exploitation, Reverse Engineering, Web Exploitation, Hardware and High Speed Computing*. Efiens Blog and Efiens CTFTime Ranking, and Efiens Achievement

I help organizing International Capture The Flag Competition in Vietnam. And it was on the news!

Learning

Individual exploration of research topics, ordered from *newest to oldest*:

- Deep Learning for Coders with fastai & PyTorch
- Slide: Automatic Heap Layout Manipulation for Exploitation
- Qiling - Advanced Binary Emulation framework
- Practical Binary Analysis
- Automate Binary Analysis, Dynamic Symbolic Execution
- Malware Data Science
- Apply Lattice to Cryptanalysis
- Generating Anomalous Elliptic Curves
- Implement Elliptice Curve attack
- Survey of attacks against RSA