Duc (Cothan) Tri Nguyen

He/Him/His
VA, USA
cothan@efiens.com
Blog
Writeup
Github
CERG Profile
Google Scholar

Graduate Research Assistant at George Mason University

Languages & Technologies

ordered by proficiency

Languages	**Python, C, C++**, Bash, VHDL, Tcl, Swift
Libraries	**Angr, Ghidra, Z3Prover, Radare2, pwntool**, Qiling, Numpy, Keras
Software	**Visual Code, GNU Debugger, x64dbg, IDA, Valgrind, Cutter,** Burp, SageMath, QEMU, Splunk
Security Skills	**Cryptography, Reverse Engineering, Binary Analysis, Binary Exploitation**
Hardware	FPGA: **Xilinx Vitis, Vivado HLx** | GPU: **OpenACC**
Assembly	AVX2, ASIMD (aarch64), x86_64, ARM

Education

Graduate Research Assistant in the area of Post-Quantum Cryptography
Electrical & Computer Engineering
George Mason University, USA
September 2017 - Present

B.S. in Computer Engineering
Computer Science and Engineering
Bach Khoa University, Vietnam
November 2015

Experiences

PhD Student - Graduate Research Assistant
CERG GMU, George Mason University
August 2017 - Present

- **FPGA Cryptographic Engineering**:
  - Evaluate, benchmark Post-Quantum Cryptography (PQC) NIST *lattice-based* candidates
  - Offload time-critical PQC functionality to FPGA
  - Design and Implement High speed Hardware architecture in High-Level-Synthesis
  - Experiment and testing result on SDSoc Platform, estimate speed-up
  - Published Round 1 PQC code: NTRUEncrypt, NTRU-HRSS, NTRU Prime
  - Design high speed, optimal latency hardware architecture for Polynomial Multiplication using Number Theoretic Transform applied to: CRYSTAL-Kyber/Dilithium, NewHope
- **Implement Post-Quantum Cryptography in SIMD**:
  - Contributed to SUPERCOP: NEON implementation of SABER
  - Project: NEON implementation of NTRU
- **Binary Analysis**:
  - Deep Learning: *Resolving disassembler architecture ambiguity using Neural Network*
  - Side channel Instruction Counter using Qiling, QEMU

Operation Security Internship
VNG Corporation,
Le Dai Hanh, Ho Chi Minh City, Vietnam
December 2014 - April 2015

- Tracked and monitored security events
- Detected and responded to abnormal activities and behavior of sophisticated malware

Publications

2020

Nguyen, D, T, Dang, V. B, & Gaj, K. *"High Level Synthesis in Implementing and Benchmarking Number Theoretic Transform in Lattice-based Post-Quantum Cryptography using Software/Hardware Codesign"*. 16th International Symposium on Applied Reconfigurable Computing, Toledo, Spain. April 1-3, 2020. (Poster)

2019

Nguyen, D, T, Dang, V. B, & Gaj, K. *"A High-Level Synthesis Approach to the Software/Hardware Codesign of NTT-based Post-Quantum Cryptography Algorithms"*. In 2019 International Conference

on Field-Programmable Technology (FPT), Tianjin, China, Dec 9-13, 2019. (Poster)

Farahmand, F., **Nguyen, D. T.**, Dang, V. B., Ferozpuri, A., & Gaj, K. (2019, September). *"Software/Hardware Codesign of the Post Quantum Cryptography Algorithm NTRUEncrypt Using High-Level Synthesis and Register-Transfer Level Design Methodologies"*. In 2019 29th International Conference on Field Programmable Logic and Applications (FPL), Barcelona, Spain, Sep. 9-13, 2019.

Banegas, G., Barreto, P. S., Boidje, B. O., Cayrel, P. L., Dione, G. N., Gaj, K., ... & **Nguyen, D. T**. (2019, May). *"DAGS: Reloaded Revisiting Dyadic Key Encapsulation"*. In Code-Based Cryptography Workshop (pp. 69-85). Springer, Cham.

Farahmand, F., Dang, V. B., **Nguyen, D. T.**, & Gaj, K. (2019, May). *"Evaluating the Potential for Hardware Acceleration of Four NTRU-Based Key Encapsulation Mechanisms Using Software/Hardware Codesign"*. In International Conference on Post-Quantum Cryptography (pp. 23-43). Springer, Cham.

2018

Banegas, G., Barreto, P. S., Boidje, B. O., Cayrel, P. L., Dione, G. N., Gaj, K., ... & **Nguyen, D. T**. *"DAGS: Key encapsulation using dyadic GS codes"*. Journal of Mathematical Cryptology, 12(4), 221-239.

Research & Learning

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

- TPM meets Timing and Lattice Attacks
- Rowhammer.js: A Remote Software-InducedFault Attack in JavaScript
- One Bit Flips, One Cloud Flops:Cross-VM Row Hammer Attacks and Privilege Escalation
- 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
- Contruct Hidden subgroup to backdoor Diffie-Hellman
- Generating Anomalous Elliptic Curves
- Implement Elliptice Curve attack
- Survey of attacks against RSA

Conferences

16th International Symposium on Applied Reconfigurable Computing (reschedule)
Toledo, Spain
April 1st - 3rd 2020

2019 International Conference on Field-Programmable Technology
Tianjin, China
December 7th - 14rd 2019

First PQC Standardization Conference
Fort Lauderdale, Florida, USA
April 11st - 13rd 2018

PQCrypto 2018
Fort Lauderdale, Florida, USA
April 9th - 11st 2018

Training

IACR-SEAMS School "Cryptography: Foundations and New Directions"
Ha Noi, Vietnam
November 27th - December 4th 2016

High-Speed Cryptography, Elliptic Curve Cryptography, Discrete Log Problem, Provable Security

Big Data and Social Analytics Certificate course
MIT Experiential Learning
August - October 2016

CIMPA-ICTP research school on Lattices and applications to cryptography and coding theory
Saigon University, Ho Chi Minh City, Vietnam.
August 1st - 12th, 2016

Number theory, Lattices and Cryptography, Elliptic Curve and Cryptography.

Machine Learning
Coursera
November - December 2015

Multivariate Linear Regression, Polynomial Regression, Gradient Descent, Cost Function, Evaluating a Hypothesis, Model selection and Train/Validation/Test Sets, Learning Curve.

Cryptography 1
Coursera
January - March 2015

Discrete Probability, Attacking Linear Pseudo Random Generator, Attacking modes of operation of block ciphers, HMAC, Key Exchange, Public Key Cryptography

Competitions

PatriotCTF George Mason University, VA, USA *April 25th 2020*	3rd / Efiens
UMDCTF University of Viginia, VA, USA *April 19th 2020*	4th / MasonCC
✹ **MACCDC 2020 Regional Final Round** *Tied for 1st place in* Services *category* *April 2nd 2020*	5th / MasonCC
International Students' Olympiad in Cryptography 2019 Novosibirsk State University, Russia *December 2nd 2019*	3rd in Professional Round
MetaCTF University of Viginia, VA, USA *November 2nd 2019*	1st / BackToBack
Pros Vs Joes BSides DC 2019, Washington DC, USA *Oct 25 2019*	2nd / Honk_Honk_Honk
VTSummit 2019 Virginia Tech - Virginia, USA *March 23rd 2019*	1st / MasonCC
UMBC Cyber Dawgs 2019 University of Maryland - Baltimore County, Maryland, USA *March 2nd 2019*	2nd / MasonCC
International Students' Olympiad in Cryptography 2018 Novosibirsk State University, Russia *December 3rd 2018*	Diploma in Professional Round
Post-Quantum Cryptography Competitions **DAGS Submission Team** NIST, USA *2017*	Round 1
International Students' Olympiad in Cryptography 2017 Novosibirsk State University, Russia *December 21st 2017*	3rd in Professional Round

2016 CTF Team Rating Overall Score *Summarized scores taking into account CTF competitions all over the world* *January 1st 2017*	**1st / DCUA**
International Students' Olympiad in Cryptography 2016 *An answer to one of the problems nominated as a best solution* Novosibirsk State University, Russia *December 14th 2016*	3rd in Professional Round
CSAW Finalist 2016 NYU Abu Dhabi, United Arab Emirates *November 11-12 2016*	1st / DCUA
ASIS Final Round 2016 Iran Cyber Security Contest *September 11st 2016*	1st / DCUA
Hack in the Box Singapore 2016 Facebook, Singapore *August 2016*	4th / DCUA
HITB CTF Amsterdam 2015 Amsterdam, The Netherlands *May 2015*	2nd / DCUA
National Cyber Security 2014 VNISA, Vietnam *November 2014*	2nd / BKIT-Respawn

Qualifications

ECSI Hacker Playground 2015
Silent Signal, Balabit IT Security
National Hero Certificate

CIMPA 2016
Mathematics school

IACR-SEAMS School 2016
Cryptography school

CSAW 2016 Finalist Certificate
NYU Abu Dhabi

International Students' Olympiad in Cryptography 2016
3rd place Diploma

International Students' Olympiad in Cryptography 2017
3rd place Diploma

International Students' Olympiad in Cryptography 2018
Diploma

International Students' Olympiad in Cryptography 2019
Diploma

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 Fanpage
- Efiens CTFTime Ranking:
  - Base on CTFTime country ranking, Efiens is top security club in Vietnam
  - Base on Cryptography competition history, Efiens is top cryptography research club in Vietnam

I didn't participate some of these events, I put it here to keep track of Efiens Achievement

International Students' Olympiad in Cryptography 2019 Novosibirsk State University, Russia *Professional Round, December 2nd 2019*	2nd, 2nd, 3rd
National Cyber Security 2019 VNISA, Vietnam *November 2019*	Finalist
Mates CTF Season 3 Viettel Cyber Security, Hanoi, Vietnam *June 29th 2019*	2nd / noobk
International Students' Olympiad in Cryptography 2018 Novosibirsk State University, Russia *Professional Round, December 3rd 2018*	2nd, 3rd, Diploma
Mates CTF Season 2 Viettel Cyber Security, Hanoi, Vietnam *August 11st 2018*	Finalist
International Students' Olympiad in Cryptography 2017 Novosibirsk State University, Russia *Professional Round, December 21st 2017*	3rd, 3rd
International Students' Olympiad in Cryptography 2016 *An answer to one of the problems nominated as a best solution* Novosibirsk State University, Russia *Professional Round, December 14th 2016*	3rd

As member of Meepwn team, I help organizing International Capture The Flag Competition in Vietnam. And it was on the news too!