Kittiphon Phalakarn

Contact Information

Engineering 7 Room 5414
Department of Electrical and Computer Engineering
University of Waterloo, Ontario, Canada

E-mail: kphalakarn@uwaterloo.ca
kittiphon.phalakarn@gmail.com
Website: https://kittiphonp.github.io/

Research Interests

- Efficient algorithms in various settings: graph algorithms, approximation algorithms
- Cryptography: post-quantum cryptography, elliptic-curve cryptography
- Formal verification: theoretical and practical verification algorithms

Education

University of Waterloo, Ontario, Canada

Ph.D. Candidate, Electrical and Computer Engineering, 2019–present
(Expected graduation date: August 2023)
Dissertation Topic: "On Parallel Computation of Large Smooth-Degree Isogeny"

Chulalongkorn University, Bangkok, Thailand

M.Eng., Computer Engineering, 2017–2019
B.Eng., Computer Engineering (First Class Honors), 2013–2017

Honors and Awards

Ripple Graduate Fellowship, 2019–2023

University of Waterloo Faculty of Engineering Graduate Scholarship, 2023

Chulalongkorn University Department of Computer Engineering Graduate Fellowship, 2017–2019

Chulalongkorn University Faculty of Engineering Gold Medal of Excellence, 2017

Outstanding Academic Performance Award, Engineering Institute of Thailand, 2016

First Solution Award in ACM-ICPC World Finals, 2016

Academic Experience

National Institute of Informatics, Tokyo, Japan

Research Intern at ERATO Metamathematics for Systems Design Project, March–August 2019

The University of Tokyo, Tokyo, Japan

Research Intern at Imai Laboratory, Department of Computer Science, June–July 2016

Teaching Experience

University of Waterloo, Ontario, Canada

Teaching Assistant

- ECE 606 Algorithm Design and Analysis, Fall 2020
- ECE 124 Digital Circuits and Systems, Spring 2020

Chulalongkorn University, Bangkok, Thailand

Teaching Assistant

- 2110201 Computer Engineering Mathematics (Linear Algebra), Winter 2019
- 2110202 Discrete Structures and Computability (Discrete Mathematics), Fall 2018
- 2110101 Computer Programming, Winter 2015, Fall 2016, Winter 2017, Spring 2017, Fall 2017, Winter 2018, Spring 2018

Peer-reviewed Publications

K. Phalakarn, V. Suppakitpaisarn, F. Rodríguez-hendríguez, and M. A. Hasan. "Vectorized and Parallel Computation of Large Smooth-Degree Isogenies using Precedence-Constrained Scheduling," IACR Trans. on Cryptographic Hardware and Embedded Systems (TCHES), vol. 2023, issue 3, pp. 246–269.

K. Phalakarn, V. Suppakitpaisarn, and M. A. Hasan. "Speeding-Up Parallel Computation of Large Smooth-Degree Isogeny Using Precedence-Constrained Scheduling," Proc. of the 27th Australasian Conference on Information Security and Privacy (ACISP 2022), pp. 309–331.

K. Phalakarn, V. Suppakitpaisarn, and M. A. Hasan. "Single-round Lattice-based Multisignatures," Proc. of the 8th International Workshop on Information and Communication Security (WICS 2021), pp. 365–371.

K. Phalakarn, T. Takisaka, T. Haas, and I. Hasuo. "Widest Paths and Global Propagation in Bounded Value Iteration for Stochastic Games," Proc. of the International Conference on Computer Aided Verification (CAV 2020), pp. 349–371.

K. Phalakarn, K. Phalakarn, and V. Suppakitpaisarn. "Optimal Representation for Right-to-Left Parallel Scalar and Multi-Scalar Point Multiplication," International Journal of Networking and Computing (IJNC), vol. 8, no. 2, July 2018, pp. 166–185.

K. Phalakarn, and A. Surarerks. "A Matrix Decomposition Method for Odd-Type Gaussian Normal Basis Multiplication," Proc. of the 3rd International Conference on Computer and Communication Systems (ICCCS 2018), pp. 99–103.

K. Phalakarn, K. Phalakarn, and V. Suppakitpaisarn. "Optimal Representation for Right-to-Left Parallel Scalar Point Multiplication," Proc. of the 4th International Workshop on Information and Communication Security (WICS 2017), pp. 482–488.

K. Phalakarn, and A. Surarerks. "An Analysis of Computer Programs using Lambda Calculus," Proc. of the 7th International Workshop on Computer Science and Engineering (WCSE 2017), pp. 214–218.

K. Phalakarn, **K. Phalakarn**, and V. Suppakitpaisarn. "Parallelized Side-Channel Attack Resisted Scalar Multiplication Using q-Based Addition-Subtraction k-chains," Proc. of the 4th International Symposium on Computing and Networking (CANDAR 2016), pp. 140–146.

Other Publications

K. Phalakarn, K. Phalakarn, S. Prasitjutrakul, and S. Sinthupinyo. "Python 101," Textbook for 2110101 Computer Programming course (in Thai), August 2017.

Skills

- Programming Languages: Python, C/C++, Java; some experience with R, VHDL, Verilog, OpenMP API for parallel programming.
- Languages: Thai (native), English (fluent), Japanese (beginner).