Curriculum Vitae

Full name:	**TRAN Duong Dinh**
Nationality:	Vietnamese
Date of birth:	
Address:	Ishikawa, Nomi
Email:	duongtd@jaist.ac.jp
Phone:	

EDUCATION

PhD Information Science
Japan Advanced Institute of Science and Technology (JAIST) 10/2020 - 09/2023

MSc Information Science
JAIST 10/2019 - 09/2020
VNU University of Engineering and Technology (VNU-UET) 10/2018 - 09/2019

BSc Information Technology 09/2014 - 05/2018
VNU University of Engineering and Technology (VNU-UET)

ACADEMIC DEGREE

PhD in Information Science
Japan Advanced Institute of Science and Technology
September 2023
Dissertation title: Formal verification with algebraic technique and its application
Supervisor: Prof. Kazuhiro Ogata

OCCUPATION

- From June, 2017 to December, 2017: Software engineer intern at Viettel Network Technologies Center, Viettel Group.
- From August, 2018 to September, 2019: Teaching Assistant at VNU-UET, Faculty of Information Technology (undergraduate courses, taught in Vietnamese and English).
- From October, 2020 to December, 2020 and from October, 2021 to December, 2021: Teaching Assistant at JAIST, Information Science school (graduate courses, taught in English).
- 10/2023 to present: Postdoctoral researcher at JAIST.

SPECIALIZED FIELDS

- Practical application of formal method to automated testing and verification of Autonomous Driving Systems (ADSs). I have developed a framework for runtime verification of ADSs, leveraging some formal method techniques.

- Application of formal verification to verification of different kinds of systems/protocols, such as classical security protocols, mutual exclusion protocols, and concurrent/distributed protocols. I have developed a tool called IPSG that automates some tedious manual tasks when doing theorem proving with CafeOBJ, an advanced specification language, and also can be used as a powerful interactive theorem proving system.
- Security analysis/verification of post-quantum cryptographic protocols, a new class/standardization of cryptographic protocols against future attacks from quantum computers.

SOCIAL ACTIVITIES

I serve as a program committee of the following conferences:

- The 25th International Conference on Formal Engineering Methods (ICFEM 2024), Hiroshima, Japan.

I serve as a reviewer of the following journals:

- Journal of King Saud University - Computer and Information Sciences (Elsevier).
- Computer Standards and Interfaces journal (Elsevier).
- Science of Computer Programming (Elsevier).

I serve as the publicity chair of the following workshops:

- The 1st International Workshop on Formal Analysis and Verification of Post-Quantum Cryptographic Protocols (FAVPQC), Madrid, Spain, 2022 (https://favpqc2022.gitlab.io).
- The 2nd FAVPQC Workshop, Brisbane, Australia, 2023 (https://favpqc2023.gitlab.io).
- The 15th International Workshop on Rewriting Logic and its Applications (WRLA), Luxembourg, 2024 (https://wrla2024.gitlab.io).

I am a reviewer of the following workshop:

- The 1st FAVPQC workshop.

AWARDS

- 09/2023: JAIST Outstanding Graduate Student Award.
- 04/2022: NEC C&C Grants for Non-Japanese Researchers from 4/2022 to 3/2023.
- 10/2020: JAIST Doctoral Research Fellowship from 10/2020 to 9/2023.
- 09/2019: Vietnam National University & JAIST 1-1 Master scholarship.
- 06/2018: The highest GPA among graduating students in the Information Technology major, Class of 2014-2018.
- 06/2018: Certificate of Merit from VNU Director "Outstanding student 2014-2018 period."
- 07/2022: JAIST Research Grants for attending the conference SEKE 2022.
- 07/2021: JAIST Research Grants for attending the conference SEKE 2021.
- 12/2020: JAIST Research Grants for attending the conference APSEC 2020.
- 07/2020: NEC C&C Grants for attending the conference SEKE 2020.

REFEREES

Prof. Ogata Kazuhiro
I97, School of Information Science,
JAIST, Ishikawa, 923-1292 Japan
Email: ogata@jaist.ac.jp
Tel: +81-761-51-1211

Assoc. Prof. Santiago Escobar
Dept. of Computer Systems and Computation, Valencia
Polytechnic University, Valencia, E-46022 Spain
Email: sescobar@upv.es
Tel: +34-96-387-7000

ACHIEVEMENTS IN EDUCATION

- Teaching Assistant of "Functional Programming", JAIST, 2021 (graduate course, in English). I assisted the professor with online lectures, such as preparing online meetings before lectures.
- Teaching Assistant of "Operating Systems", JAIST, 2020 (graduate course, in English). I prepared weekly assignments & examination tests (both middle and final), graded students' assignments & examination tests, and held tutorial hours for discussion.
- Lecturer at VNU University of Engineering and Technology (Vietnam) from 08/2018 to 09/2019, teaching two courses:
  - Object Oriented Programming (undergraduate course, taught in Vietnamese and English): I was in charge of holding weekly practical programming lessons, where I directly assisted undergraduate students to practice programming in Object Oriented concepts (in Java).
  - Advanced Programming (undergraduate course, taught in Vietnamese and English): I was in charge of holding weekly practical programming lessons, where I directly assisted undergraduate students to practice programming (in C++).

ACHIEVEMENTS IN RESEARCH

Refereed Journal papers:

1. Duong Dinh Tran, Kazuhiro Ogata, Santiago Escobar, Sedat Akleylek, and Ayoub Otmani. Formal Analysis of Post-Quantum Hybrid Key Exchange SSH Transport Layer Protocol. *IEEE Access*, Vol. 12, pp. 1672-1687, 2023, doi: 10.1109/ACCESS.2023.3347914.

   We construct a symbolic model of a proposed quantum-resistant version of the SSH Transport Layer protocol, specify it in the specification language CafeOBJ, and conduct a formal analysis of the claimed security properties. Three security properties are formally verified, while with another property, namely authentication, we find a counterexample against it, and then we propose to slightly revise the protocol. With the improved version, we formally verify that the authentication property is met.

2. Duong Dinh Tran, Canh Minh Do, Santiago Escobar, and Kazuhiro Ogata. Hybrid post-quantum Transport Layer Security formal analysis in Maude-NPA and its parallel version, *PeerJ Computer Science*, Volume 9, 2023, doi: 10.7717/peerj-cs.1556.

   This paper presents a security analysis of the Hybrid Post-Quantum TLS protocol, a post-quantum version of TLS proposed by AWS. The security properties under analysis are the secrecy of the shared key established between two honest participants with the classical key exchange algorithm, a similar secrecy property but with the post-quantum key encapsulation mechanism, and the authentication property.

3. Dang Duy Bui, Duong Dinh Tran, Kazuhiro Ogata, and Adrian Riesco. Integration of state machine graphical animation and Maude to facilitate characteristic conjecture: An approach to lemma discovery in theorem proving, *Multimedia Tools and Applications*, 2023, doi: 10.1007/s11042-023-15780-5.

   We integrate the visualization tool SMGA and Maude, a declarative language and high-performance tool so that the revised version r-SMGA can use some powerful features of Maude, such as parsing associative-commutative binary operators as well as context-free grammars, and reachability analysis.

4. Duong Dinh Tran, Kazuhiro Ogata, Santiago Escobar, Sedat Akleylek, and Ayoub Otmani. Kyber, Saber, and SK-MLWR lattice-based key encapsulation mechanisms model checking with Maude. *IET Information Security*, Vol. 2023, 2023. doi: 10.1049/2023/9399887.

5. Duong Dinh Tran, Thet Wai Mon, and Kazuhiro Ogata. Transport Layer Security 1.0 handshake protocol formal verification case study: How to use a proof script generator for existing large proof scores, *PeerJ Computer Science*, Volume 9, 2023, doi: 10.7717/peerj-cs.1284.

6. Duong Dinh Tran and Kazuhiro Ogata. Formal verification of TLS 1.2 by automatically generating proof scores, *Computers & Security*, Volume 123, 2022, doi: 10.1016/j.cose.2022.102909.

   This paper proposes an approach and implements a tool supporting it, called Invariant Proof Score Generator, that can automatically generate formal proofs, called proof scores, for formal verification of invariant properties. The efficiency and the practicability of the tool are demonstrated with various systems/protocols, such as mutual exclusion protocols and real cryptographic protocols currently in use.

7. Duong Dinh Tran, Dang Duy Bui and Kazuhiro Ogata. Simulation-Based Invariant Verification Technique for the OTS/CafeOBJ Method, *IEEE Access*, Volume 9, pp. 93847-93870, 2021, doi: 10.1109/ACCESS.2021.3093211.

   We demonstrate the power of the simulation-based invariant verification technique through two case studies in which it is formally verified that two mutual exclusion protocols, MCS protocol and Anderson protocol, enjoy the mutual exclusion property by the simulation-based invariant verification technique.

Refereed Conference and Workshop papers:

- Buntita Sriarunothai, Chutikarn Kamsem, Phaiboon Jaradnaparatana, Supithcha Jongphoemwatthanaphon, Burit Sihabut, Duong Dinh Tran, and Toshiaki Aoki. Bridging Gaps between Scenario-Based Safety Analysis and Simulation-based Testing for Autonomous Driving Systems, in The Workshop on Emerging Technologies in Dependable, Secure, Autonomous Systems (PRDC'24 Workshop), to appear.
- Duong Dinh Tran and Kazuhiro Ogata. Verifying Safe Memory Reclamation in Concurrent Programs with CafeOBJ, in the 15th International Workshop on Rewriting Logic and its Applications (WRLA), 2024, pp. 45-61, doi: 10.1007/978-3-031-65941-6_3.
- Duong Dinh Tran, Kazuhiro Ogata, and Santiago Escobar. A formal analysis of OpenPGP's post-quantum public-key algorithm extension, in *the 2nd International Workshop on Formal Analysis and Verification of Post-Quantum Cryptographic Protocols*, 2023.
- Duong Dinh Tran and Kazuhiro Ogata. IPSG: Invariant Proof Score Generator, in the *IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC)*, 2022, pp. 1050-1055, doi: 10.1109/COMPSAC54236.2022.00164.
- Duong Dinh Tran, Kazuhiro Ogata, Santiago Escobar, Sedat Akleylek, and Ayoub Otmani. Formal specification and model checking of Saber lattice-based key encapsulation mechanism in Maude, in *The 32nd International Conference on Software Engineering and Knowledge Engineering (SEKE)* 2022, doi: 10.18293/SEKE2022-097.
- Dang Duy Bui, Duong Dinh Tran, Kazuhiro Ogata, and Adrian Riesco. Integration of SMGA and Maude to Facilitate Characteristic Conjecture, in *International DMS Conference on Visualization and Visual Languages (DMSVIVA)* 2022, doi: 10.18293/DMSVIVA22-006.
- Duong Dinh Tran, Kentaro Waki, and Kazuhiro Ogata. Formal specification and model checking of a recoverable wait-free version of MCS, in *SEKE* 2021, doi: 10.18293/SEKE2021-065.
- Thet Mai Won, Duong Dinh Tran, and Kazuhiro Ogata. Formal verification of IFF and NSLPK authentication protocols with CiMPG, in *SEKE* 2021, doi: 10.18293/SEKE2021-037.
- Minxuan Liu, Dang Duy Bui, Duong Dinh Tran, and Kazuhiro Ogata. Formal Specification and Model Checking of an Autonomous Vehicle Merging Protocol, Proc. *IEEE 21st International Conference on Software Quality, Reliability and Security (QRS)*, 2021, pp. 333-342, doi: QRS-C55045.2021.00057.
- Duong Dinh Tran, Dang Duy Bui, Parth Gupta, and Kazuhiro Ogata. Lemma Weakening for State Machine Invariant Proofs, in the *27th Asia-Pacific Software Engineering Conference (APSEC)*, 2020, pp. 21-30, doi: 10.1109/APSEC51365.2020.00010.
- Duong Dinh Tran and Kazuhiro Ogata. Formal verification of an abstract version of Anderson protocol with CafeOBJ, CiMPA and CiMPG, in *SEKE*, 2020, doi: 10.18293/SEKE2020-064.
- Duong Dinh Tran and Kazuhiro Ogata. Formal verification of an abstract version of Anderson protocol with CafeOBJ, CiMPA and CiMPG, Proc. *32nd International Conference on Software Engineering and Knowledge Engineering*, 2020, pp. 287-292, doi: 10.18293/SEKE2020-064.

For the full publications, please see: https://scholar.google.com/citations?user=VnWazk8AAAAJ.

OTHER ACTIVITIES RELATED TO EDUCATION AND RESEARCH

I have been employed as a researcher in the following two research projects:

- **Formal Analysis and Verification of Post-Quantum Cryptographic Protocols**, from April 2021 to March 2024. This is an internationally collaborative project investigated by Santiago Escobar, Ayoub Otmani, Sedat Akleylek, and Kazuhiro Ogata from Spain, France, Turkey, and Japan, respectively (see https://www.jst.go.jp/inter/english/program_e/multilateral_e/concert-japan.html). This project aims to formally analyze the security of *post-quantum cryptographic protocols*, a new class of cryptographic protocols against future attacks from quantum computers. With the rapid development of quantum computers and advance in quantum computing in recent years, standardization of such protocols and security analysis of them are indeed indispensable. As part of this project, I developed a tool called Invariant Proof Score Generator (IPSG) that automates some tedious manual tasks when doing verification of cryptographic protocols with CafeOBJ specification language. We have published several papers in some international conferences and journals reporting our analysis results.
- **Formal Methods and Verification Tools for Next-generation Automotive System Platforms**, from June 2024 to present. This project is funded by CREST and investigated by Toshiaki Aoki, Daisuke Ishii, and Takashi Tomita from JAIST (see https://www.jst.go.jp/kisoken/crest/en/project/1111114/1111114_2023.html). The project's goal is to propose formal methods and verification tools to ensure the safety and reliability of next-generation automotive system platforms. As part of my contributions, so far, I have developed a runtime verification framework, comprising of AWSIM-Script, a scripting language for defining traffic scenarios; Runtime Monitor, a tool to record real-time data during the simulation for offline verification; and AW-Checker, a Linear Temporal Logic-based property checker for verifying safety requirements.

RESEARCH PLAN

Formal Methods for Ensuring Safe and Reliable Autonomous Driving Systems.

Ensuring the reliability of Autonomous Driving Systems (ADSs), a promising future mode of transportation, poses significant challenges due to the complexity of these systems. Formal methods play a crucial role in addressing these challenges by providing a rigorous approach to guaranteeing the absence of undesirable behaviors in these systems.

My research focuses on the practical application of formal methods for verifying ADSs to ensure their safe and reliable operation under diverse driving conditions. A scenario-based approach, which systematically breaks the testing and verification space into manageable scenarios, shows significant promise in this context. While numerous studies have explored scenario-based testing and verification of ADSs, most focus on identifying critical scenarios that pose significant risks or could lead to collisions. Although these approaches are effective for detecting high-risk scenarios, they cannot guarantee comprehensive coverage of all potential cases. To overcome this limitation, my research will leverage well-established ADS safety standards, which offer a structured and systematic methodology for conducting thorough safety analyses. A key challenge in this approach lies in managing the large number of scenarios required for such comprehensive verification. Formal method techinques like model checking can provide significant advantages in addressing this challenge by systematically exploring these scenarios.

ADSs are inherently complex, integrating various technologies across multiple subcomponents, such as the perception module and control systems. My research will address both system-level verification (e.g., collision avoidance) and component-level verification (e.g., the precision of the perception module in detecting surrounding vehicles). Component-level verification is particularly critical, as identifying undesired behaviors at the system level often makes it difficult to pinpoint the root cause or the specific module responsible for the fault.