CHAN NGO

+33 (0)651 766 636 ◇ chan.ngo2203@gmail.com ◇ van-chan.ngo(Skype)
263 avenue General Leclerc, 35042 Rennes, France
https://fr.linkedin.com/in/channgo2203

EDUCATION

INRIA, Rennes, France *August 2014*
Ph.D in Computer Science & Engineering
Programming Language, Compiler, and Formal Verification for Embedded and Safety-Critical Systems
First Class Honors

Université Joseph Fourier, VERIMAG, Grenoble, France *June 2008*
Masters in Computer Science & Engineering
Embedded Software and Systems
French Government Scholarship, Évariste Galois Program

Hanoi University of Technology, Hanoi, Vietnam *July 2005*
Engineer Degree in Computer Engineering
Information Systems and Communication, Centre of Talented Training - PFIEV
First Class Honors with Congratulations of the Ministry of Education

EXPERIENCE

Carnegie Mellon University *2016 - Present*
Research Fellow, Computer Science *Pittsburgh, PA, US*

- Resource bounds (time, memory, ...) static analysis of imperative programs for detecting security vulnerability (time side-channel attacks, stack overflow,...)
- Probabilistic assertion checking of probabilistic programming

INRIA France *2014 - 2015*
R&D Engineer *Rennes, France*

- Design and implementation tools applying Statistical Model Checking for SystemC models
- Realization of High-Level Petri Net models in SystemC for performance analysis of microprocessor designs at level of transactions
- Probabilistic temporal assertion-based verification of SystemC models

INRIA France *2011 - 2014*
Research Assistant *Rennes, France*

- Correctness of the highly optimizing and industrial synchronous compiler, Signal, which is used in model-based design of real-time and safety-critical systems. Implement the verification framework in OCaml and C++
- Methodology of verification based on the translation validation approach by generating the formal models of clock semantics, data dependencies and value-equivalence for source code program and the compiled program. Then, using several techniques including model checking, theorem proving, graph transformation to prove the preservations of clock semantics, data dependencies and value-equivalence of variables
- Teaching Object-Oriented Programming in C++ and formal methods

Tech Propulsion Lab USA *2010 - 2011*
Software Architect *Saigon Branch, Vietnam*

- Design and development of embedded mobile software
- Technical designs of mobile applications on iOS and Android
- Project management in the mobile development department

IBM Zurich Lab and ZISC *2008 - 2010*
Research Assistant *Zurich, Switzerland*

- Formally verifying and certifying the design of secure boot processes in IBM mainframes
- Methodology of verification by generating the formal models of the boot processes using the language of the model checker Spin. The formal models are used to verify the security properties of the boot process. This work is applied on the AIX mainframes of IBM

VERIMAG Lab *2007 - 2008*
Internship *Grenoble, France*

- A general framework to verify automatically the secure property IND-CPA property of asymmetric encryption schemes, to be suitable for computer tools
- Automated verification framework to prove formally the IND-CPA security property of asymmetric encryption schemes. The framework represents the encryption schemes as *frame* in cryptographic π-calculus, and formalize the IND-CPA property as a equivalent relation between two frames

IBM Vietnam *2006 - 2007*
Senior Software Engineer *Hanoi, Vietnam*

- Working on text search engine of data base management DB2 of IBM

FPT Software *2005 - 2006*
Software Engineer *Hanoi, Vietnam*

- Working on embedded systems for navigation

Security Systems, MISOFT *2003 - 2005*
Software Developer *Hanoi, Vietnam*

- Developing a distributed firewall as an operation system based on the package filtering library and the Linux kernel in C++ and Python

Hanoi University of Technology *2000 - 2003*
Tutor *Hanoi, Vietnam*

- Student teaching in Mathematics and Physics

TECHNICAL STRENGTHS

- **Programming Languages**: Assembly, C/C++/C♯, Ada, Java, OCaml and Python

- **Programming Tools**: GCC Toolchain, LLVM, XCode, Visual Studio, Eclipse, IAR Workbench, AVR Studio, Arduino IDE, SVN, Git

- **Embedded Software Development**: RTLinux, FreeRTOS, Assembly, C/C++, and Ada for AVR, ARM, and Arduino Development Boards

- **Formal Methods & Modeling Languages**: SystemC, System Verilog, Automata, Label Transition System (State Machine), Markov Chains, Petri Nets, Synchronous Languages (Signal, Lustre and

Esterel/Scade), Logics and Temporal Logics (LTL, CTL, Specification Languages SVA and PSL), Abstraction Interpretation, Model Checking, Theorem Proving, Static Analysis

- **Formal Method Tools**: SPIN, SMV, UPAAL, PRISM, SMC Plasma Lab, SAT/SMT Solvers, Coq Proof Assistant, Frama-C, Why3, Synopsys Design Compiler

LANGUAGES

English - Advance **French** - Advance **Vietnamese** - Mother-tongue

INTERESTS

Instrumental Painting Running Photography Cooking Robotic

AWARDS

Ph.D scholarship, INRIA France
DEA scholarship from the French government, Université Joseph Fourier, France
Masters scholarship from the Italian government, Politecnico di Milano, Italy
Masters scholarship from SamSung company, ICU-KAIST, South Korea
Scholarships from Hanoi University of Technology for excellent academic results

SOFTWARES

- **SysCPlasma**: Formal Verification of SystemC Models with Statistical Model Checking. It consists of two components: the plugin for Plasma Lab in Java, SystemC Plugin, and tool for generating monitor and aspect advices in C++, MAG

- **Plasma Lab**: Plasma Lab is a compact, efficient and flexible platform for statistical model checking of stochastic models

- **Polychrony**: The Polychrony toolset developed in C++ and Java, based on Signal, provides a formal framework to design, develop and validate critical systems, from abstract specification until deployment on distributed systems

- **SigCert**: The tool developed in OCaml checks the correctness of the compilation of Signal compiler w.r.t clock semantics, data dependence, and value-equivalence (not fully implemented)

- **SigCV**: PDS Simulation Relation Checking with Sigali: implementation of the theory works in IFM 2012 article as the libraries in Sigali toolset

- **Mobile Apps**: Mobile applications: RATP, Turnstone, Saigon Places, A86, PhotoEnc,...on Apple App Store

RESEARCH PROJECTS

DANSE

- *Summary*: DANSE focuses on the development of a new methodology to support evolving, adaptive and iterative System of Systems (SoS) life-cycle models based on a formal semantics for SoS inter-operations and supported by novel tools for analysis, simulation, and optimisation.

  DANSE includes industrial representatives with focus on aerospace, land, and automotive systems, as well as a leading tools and framework provider in the system space, and top European research institutes in system engineering. These partners have deep interest in the outcome of the research and are eager to deploy the developments as soon as they become available.
- *Link*: http://www.danse-ip.eu/home/

DALI

- *Summary*: The DALI project has undertaken a challenging agenda aimed at extending the people autonomous life beyond the home. The environment where the system operates is partially known (due to its large variability) and changing. Our assisted living device system must therefore acquire dynamic information about the user's immediate environment in order to guide its decision-making. The construction of a system of such complexity represents a major scientific and technological effort bringing together expertise across different disciplines.
- *Link*: http://www.ict-dali.eu/dali/

VERISYNC

- *Summary*: The project proposed here aims at substantially improving the safety and reliability of embedded software that is being developed in the context of a Model-based design approach. This is achieved by formally proving the correctness of essential transformations that a model undergoes during its compilation to executable code. The definition of the semantics and the correctness proof of the compiler will be carried out by means of theorem proving. The compiler is executable and will be evaluated on realistic examples.

  The project is targeted at the compilation of a synchronous language to an imperative programming language. Synchronous languages have turned out to be an expressive formalism for embedded algorithms, and their precise semantics make them particularly suitable for our purpose.
- *Link*: http://www.irit.fr/~Martin.Strecker/Proj/Old/Verisync/

SCALP

- *Summary*: Our day-to-day lives increasingly depend upon information and our ability to manipulate it securely. That is, in a way that prevents malicious elements to subvert the available information for their own benefits. This requires solutions based on cryptographic systems (primitives and protocols). However, no matter how carefully crafted cryptographic systems are, experience has shown that effective attacks can remain hidden for years. This may be caused by poor design or often unclear and poorly defined security properties and assumptions.

  Therefore, provable security, where new systems are published with a rigorous definition of their security goals and a mathematical proof that they meet their goals, is being increasingly advocated. While the adoption of provable security significantly increases, the complexity and diversity of designed systems tend to increase too. Hence, it is largely agreed on that the point has been reached where it is no longer viable to construct or verify cryptographic proofs by hand (Bellare & Rogaway 2004, Shoup 2004, Halevi 2005) and that there is a need for computer-aided verification methods for cryptographic systems. The goal of this project is to achieve a major step towards building automated tools for the verification of cryptographic systems. In order, to reconcile generality, imposed by the high diversity of cryptographic systems, and automation, we shall build our tools upon Coq.
- *Link*: http://scalp.gforge.inria.fr/

AVOTE

- *Summary*: Electronic voting promises the possibility of a convenient, efficient and secure facility for recording and tallying votes. However, the convenience of electronic elections comes with a risk of large-scale fraud and their security has seriously been questioned. In this project we propose to use formal methods to analyze electronic voting protocols.
- *Link*: http://www-verimag.imag.fr/AVOTE.html

PUBLICATIONS

Journals and Conferences

· V.C. Ngo, A. Legay, and J. Quilbeuf. *Statistical Model Checking for SystemC Models.* In Proceedings of 17th High Assurance Systems Engineering Symposium (**HASE'16**), IEEE, Orlando, Florida, USA, January 2016

· V.C. Ngo, J-P. Talpin, T. Gautier, L. Besnard, and P. Le Guernic. *Modular Translation Validation of a Full-sized Synchronous Compiler using Off-the-shelf Verification Tools.* In Journal of Automated Reasoning (**JAR'15**), Springer, 2015 (Under Review)

· V.C. Ngo, J-P. Talpin, T. Gautier, L. Besnard, and P. Le Guernic. *Modular Translation Validation of a Full-sized Synchronous Compiler using Off-the-shelf Verification Tools.* In Proceedings of International Workshop on Software and Compilers for Embedded Systems (**SCOPES'15**), Invited Presentation, ACM, St. Goar, Germany, June 2015

· V.C. Ngo, J-P. Talpin, and T. Gautier. *Translation Validation for Synchronous Data-flow Specification in the Signal Compiler.* In Proceedings of 35th IFIP International Conference on Formal Techniques for Distributed Objects, Components and Systems (**FORTE-DisCoTec'15**), IFIP, Grenoble, France, June 2015

· V.C. Ngo, J-P. Talpin, T. Gautier, and P. Le Guernic. *Translation Validation for Clock Transformations in a Synchronous Compiler.* In Proceedings of 18th International Conference on Fundamental Approaches to Software Engineering (**FASE-ETAPS'15**), Springer, London, UK, April 2015

· V.C. Ngo, J-P. Talpin, and T. Gautier. *Precise Deadlock Detection for Polychronous Data-flow Specifications.* In Proceedings of the Electronic System Level Synthesis Conference (**ESLsyn-DAC'14**), IEEE, San Francisco, CA, USA, June 2014

· V.C. Ngo, J-P. Talpin, T. Gautier, P. Le Guernic, and L. Besnard. *Formal Verification of Synchronous Data-flow Program Transformations Toward Certified Compilers.* In Frontiers of Computer Science (**FCS'13**), Special Issue on Synchronous Programming, Springer, 2013

· V.C. Ngo, J-P. Talpin, T. Gautier, P. Le Guernic, and L. Besnard. *Formal Verification of Automatically Generated C-code from Polychronous Data-flow Equations.* Accepted at IEEE International High-Level Design, Validation and Test Workshop (**HLDVT'12**), IEEE, California, USA, November 2012

· V.C. Ngo, J-P. Talpin, T. Gautier, P. Le Guernic, and L. Besnard. *Formal Verification of Compiler Transformations on Polychronous Equations.* In Proceedings of 9th International Conference on Integrated Formal Methods (**IFM'12**), Springer, Pisa, Italy, June 2012

· C. Ene, Y. Lakhnech, and V.C. Ngo. *Formal Indistinguishability Extended to the Random Oracle Model.* In Proceedings of 14th European Symposium on Research in Computer Security (**ESORICS'09**), Springer, Saint Malo, France, September 2009 (main author)

· C. Ene, Y. Lakhnech, and V.C. Ngo. *Formal Indistinguishability Extended to the ROM.* In Proceedings of Workshop on Formal and Computational Cryptography (**FCC'09**), New York, USA, July 2009 (main author)

Thesis

· V.C. Ngo. *Formal Verification of a Synchronous Data-flow Compiler: from Signal to C.* In **Ph.D Thesis** in Computer Science, INRIA France, University of Rennes, France, July 2014

· V.C. Ngo. *Automated Verification of Asymmetric Encryption.* In **M.Sc Thesis** in Computer Science and Applied Mathematics, VERIMAG, University of Grenoble, France, June 2008

· V.C. Ngo. *Theory and Implementation of Distributed Firewall on Linux Environment* (in Vietnamese). In **Engineer Thesis** in Computer Engineerings, Center for Talent Training, Hanoi University of Technology, Vietnam, July 2005

Technical Reports

· V.C. Ngo, A. Legay, and J. Quilbeuf. *Dependability Analysis of Embedded Control Systems Using SystemC and Statistical Model Checking.* In HAL - INRIA, **Technical Report RR-8762**, July 2015

· V.C. Ngo, A. Legay, and J. Quilbeuf. *Dynamic Verification of SystemC Specification with Statistical Model Checking.* In HAL - INRIA, **Technical Report RR-8644**, October 2014

· V.C. Ngo, J-P. Talpin, T. Gautier, and P. Le Guernic. *Evaluating SDVG Translation Validation: from Signal to C.* In HAL - INRIA, **Technical Report RR-8508**, March 2014

· V.C. Ngo, J-P. Talpin, and P. Le Guernic. *Formal Verification of Transformations on Abstract Clocks in Synchronous Compilers.* In HAL - INRIA, **Technical Report RR-8064**, September 2012

· V.C. Ngo, J-P. Talpin, T. Gautier, P. Le Guernic, and L. Besnard. *Formal Verification of Synchronous Data-flow Compilers.* In HAL - INRIA, **Technical Report RR-7921**, April 2012

TALKS

- Translation Validation for Synchronous Data-flow Specification in the SIGNAL Compiler. Talk at FORTE - DisCoTec 2015, Grenoble, France, June 2015

- Translation Validation for Clock Transformations in a Synchronous Compiler. Talk at FASE - ETAPS 2015, London, UK, April 2015

- Case Study: Dependability Analysis of Embedded Control Systems using SystemC and Statistical Model Checking. Talk at INRIA Rennes, France, March 2015

- Precise Deadlock Detection for Polychronous Data-flow Specifications. Talk at ESLsyn - DAC 2014, San Francisco, CA, USA, June 2014

- Seminar: Compilation and Execution of Streaming Programs. St Germain au Mont d'Or, France, April 2014

- Formal Verification of Transformations on Clocks in Synchronous Data-flow Compilers. Talk at 19th Open International Workshop on Synchronous Programming 2012, Le Croisic, France, November 2012

- Formal Verification of Transformations on Clocks in Synchronous Data-flow Compilers. Invited Talk at Beihang University (BUAA), Beijing, China, October 2012

- Formal Verification of Compiler Transformations on Polychronous Equations. Talk at IFM 2012, Pisa, Italy, June 2012

- Formal Indistinguishability Extended to the Random Oracle Model. Talk at ESORICS 2009, Le Croisic, France, September 2009

REFEREES

- Jean-Pierre Talpin
  Research Director,
  TEA: Time, Events and Architectures Group, INRIA Rennes, Campus de Beaulieu, 263 Avenue General Leclerc, 35042 Rennes, France
  Email: Jean-Pierre.Talpin@inria.fr
  Tel: +33 (0)2 99 84 74 36
- Thierry Gautier
  Senior Researcher,
  TEA: Time, Events and Architectures Group, INRIA Rennes, Campus de Beaulieu, 263 Avenue General Leclerc, 35042 Rennes, France
  Email: Thierry.Gautier@inria.fr
  Tel: +33 (0)2 99 84 72 43
- Loïc Besnard
  Research Engineer,
  IRISA Rennes, Campus de Beaulieu, 263 Avenue General Leclerc, 35042 Rennes, France
  Email: Loic.Besnard@irisa.fr
  Tel: +33 (0)2 99 84 72 43