Chitchanok Chuengsatiansup

Post-doctoral researcher (Inria & ENS de Lyon)
https://perso.ens-lyon.fr/chitchanok.chuengsatiansup

Contact Information

École Normale Supérieure de Lyon
Laboratoire de l'Informatique du Parallélisme (LIP)
46 Allée d'Italie 69364 Lyon Cedex 07
France
E-mail: *chitchanok.chuengsatiansup@ens-lyon.fr*

Current Employment

Starting May 2017, I have been working as a post-doctoral researcher at Inria in LIP laboratory, ENS de Lyon, France. I am a member of Crypto group in Arithmetic and Computing research team. In particular, I work with Damien Stehlé on project RISQ (Regroupement de l'Industrie française pour la Sécurité post-Quantique) which concerns post-quantum cryptography.

Educational Background

Eindhoven University of Technology, The Netherlands *2013–2017*
Cryptographic Implementations Group
Department of Mathematics and Computer Science
(Graduated March 16th, 2017)
· PhD student
· Thesis: *"Optimizing Curve-Based Cryptography"* [PDF]
· Supervisors: Daniel J. Bernstein and Tanja Lange

The University of Tokyo, Japan *2010–2013*
Imai's Laboratory
Department of Computer Science
Graduate School of Information Science and Technology
(Graduated March 25th, 2013)
· Japanese Government Scholar (Monbukagakusho)
· Master's Program in Computer Science
· Thesis: *"Improved Elliptic Curve Arithmetic by Reordering Operation Sequences"* [PDF]
· Supervisor: Hiroshi Imai

Chulalongkorn University, Thailand *2006–2010*
Department of Computer Engineering
Faculty of Engineering
(Graduated April 5th, 2010)
· Bachelor of Engineering Program in Computer Engineering
· First Class Honors
· Graduation Project: *"How to Write Best Paper: An Approach to Mining Characteristics of Good Papers"*
· Supervisor: Boonserm Kijsirikul

Research Activities

Post-doctoral researcher *2017–present*
LIP laboratory
Inria and ENS de Lyon, France
Member of Crypto group in AriC team
Research theme: post-quantum cryptography

PhD student *2013–2017*
Department of Mathematics and Computer Science
Eindhoven University of Technology, The Netherlands
Member of Cryptographic Implementations group
Research theme: curve-based cryptography and cryptographic optimizations

Master's student *2011–2013*
Department of Computer Science
Graduate School of Information Science and Technology
The University of Tokyo, Japan
Member of Imai's Laboratory
Research theme: elliptic-curve cryptography

Research student *2010–2011*
Department of Computer Science
Graduate School of Information Science and Technology
The University of Tokyo, Japan
Member of Imai's Laboratory
Research theme: computational complexity

Bachelor's student *2006–2010*
Department of Computer Engineering
Faculty of Engineering
Chulalongkorn University, Thailand
Member of Engineering Innovator Club
Research theme: artificial intelligence

Research Interests

· Elliptic- and Hyperelliptic-Curve Cryptography
· Post-Quantum Cryptography
· Lattice-Based Cryptography
· Side-Channel Analysis
· Security and Privacy
· Secure Messaging

Teaching Experience

Tutoring the course "Probability" *2018*
I was in charge of the tutorials (32 hours) for *Probability* course given to 3rd-year bachelor students in Computer Science at ENS de Lyon, France.

Lecturing "Introduction to Cryptography" *2015*
During my PhD study, I was invited to give a 3-hour lecture on cryptography to Master's students in Computer Science/Engineering at Chulalongkorn University, Thailand.

Lecturing "Java Programming" *2007*
I lectured 30 hours on Java programming to middle and high school students in Thailand.

Tutoring "C Programming" *2004*
I gave a 3-hour tutorial on C programming to high school students at Triam Udom Suksa School, Bangkok, Thailand.

Tutoring "Advanced Calculus" *2004*
I gave a 6-hour tutorial on university-level calculus to high school students at Bullitt East High School, Mount Washington, Kentucky, USA.

Lecturing "C Programming" *2002*
I lectured 30 hours on C programming to middle school students at Patumwan Demonstration School, Srinakharinwiron University, Bangkok, Thailand.

Supervision Experience

I co-supervised the following Master's students:
· Sebastian Verschoor, on software implementations of Curve41417 on Haswell *2014–2016*
· Wouter de Groot, on software implementations of X25519 on Cortex M3 *2015*

Research Visits

· Monash University, Australia. (hosted by Amin Sakzad and Ron Steinfeld) *June, 2018*
· Monash University, Australia. (hosted by Amin Sakzad and Ron Steinfeld) *February, 2018*
· Kyushu University, Japan. (hosted by Tsuyoshi Takagi) *February, 2017*
· University of California, Davis, USA. (hosted by Phillip Rogaway) *August, 2016*
· National Institute of Informatics, Japan. (hosted by Vorapong Suppakitpaisarn) *March, 2015*

Program committees and reviewing articles

I was a member of the program committees for
· Australian Workshop on Offensive Cryptography — Kangacrypt 2018
· The 38th Annual International Cryptology Conference — Crypto 2018

I reviewed articles for the following journal, conferences, workshops, and symposiums:
· Journal of Cryptographic Engineering
· The 24th Annual International Conference on the Theory and Applications of Cryptology and Information Security — Asiacrypt 2018
· The 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques — Eurocrypt 2018
· The Fifth International Symposium on Computing and Networking — CANDAR 2017
· The Fifth International Conference on Cryptology and Information Security in Latin America — Latincrypt 2017
· The 23rd Annual International Conference on the Theory and Applications of Cryptology and Information Security — Asiacrypt 2017
· IEEE International Symposium on Hardware Oriented Security and Trust — HOST 2017
· The 20th Design, Automation and Test in Europe — DATE 2017
· The 12th Algorithmic Number Theory Symposium ANTS-XII — ANTS 2016
· The 19th International Conference on the Theory and Practice of Public-Key Cryptography — PKC 2016

· The 22nd International Conference on Selected Areas in Cryptography — SAC 2015
· The 21st International Conference on Selected Areas in Cryptography — SAC 2014
· The 16th Workshop on Cryptographic Hardward and Embedded System — CHES 2014

Honors & Awards (selected)

iDASH Competition
· Winner of the iDASH Genome Privacy Challenge (Track 1), 2017

Academic Excellence
· Japanese government scholarship (Monbukagakusho: MEXT), 2010–2013
· Dean's list of distinguished students (Faculty of Engineering, Chulalongkorn University), 2006–2010
· Best student award (Chulalongkorn University), 2009

Robotics
· First place in Soccer Small Size League of the 12th RoboCup World Championship, 2008
· First place in Soccer Junior League of RoboCup Thailand Championship, 2008

Applications on Mobile Phone
· Second runner-up in SAMART innovation awards (game application "Accelero Mazer"), 2008
· Consolation prize in SAMART innovation awards (analysis of behaviors on mobile usage), 2007

Language Skills

· Thai (fluent, native)
· English (fluent)
· Japanese (very good)
· French (good)
· Dutch (intermediate)
· German and Mandarin (basic)

List of publications and presentations

Chitchanok Chuengsatiansup

International Conferences with Referees

- Chitchanok Chuengsatiansup, and Chloe Martindale. *"Pairing-friendly twisted Hessian curves"*. Debrup Chakraborty and Tetsu Iwata, editors. Progress in Cryptology — INDOCRYPT 2018. Lecture Notes in Computer Science, Vol. 11356, pp. 228–247. Springer (2018). [PDF]
- Daniel J. Bernstein, Chitchanok Chuengsatiansup, Tanja Lange, and Christine van Vredendaal. *"NTRU Prime: reducing attack surface at low cost"*. Carlisle Adams and Jan Camenisch, editors. Selected Areas in Cryptography — SAC 2017. Lecture Notes in Computer Science, Vol. 10719, pp. 235–260. Springer (2018). [PDF]
- Daniel J. Bernstein, Tung Chou, Chitchanok Chuengsatiansup, Andreas Hülsing, Eran Lambooij, Tanja Lange, Ruben Niederhagen, and Christine van Vredendaal. *"How to manipulate curve standards: a white paper for the black hat"*. Liqun Chen and Shin'ichiro Matsuo, editors. Security Standardisation Research — SSR 2015. Lecture Notes in Computer Science, Vol. 9497, pp. 109–139. Springer (2015). [PDF]
- Daniel J. Bernstein, Chitchanok Chuengsatiansup, David Kohel, and Tanja Lange. *"Twisted Hessian curves"*. Kristin Lauter and Francisco Rodríguez-Henríquez, editors. Progress in Cryptology — LATINCRYPT 2015. Lecture Notes in Computer Science, Vol. 9230, pp. 269–294. Springer (2015). [PDF]
- Daniel J. Bernstein, Chitchanok Chuengsatiansup, Tanja Lange, and Peter Schwabe. *"Kummer strikes back: new DH speed records"*. Palash Sarkar and Tetsu Iwata, editors. Advances in Cryptology — ASIACRYPT 2014. Lecture Notes in Computer Science, Vol. 8873, pp. 317–337. Springer (2014). [PDF]
- Daniel J. Bernstein, Chitchanok Chuengsatiansup, and Tanja Lange. *"Curve41417: Karatsuba revisited"*. Lejla Batina and Matthew Robshaw, editors. Cryptographic Hardware and Embedded Systems — CHES 2014. Lecture Notes in Computer Science, Vol. 8731, pp. 316–334. Springer (2014). [PDF]
- Chitchanok Chuengsatiansup, Michael Naehrig, Pance Ribarski, and Peter Schwabe. *"PandA: Pairings and Arithmetic"*. Zhenfu Cao and Fangguo Zhang, editors. Pairing-Based Cryptography — Pairing 2013. Lecture Notes in Computer Science, Vol. 8365, pp. 229–250. Springer (2014). [PDF]
- Chitchanok Chuengsatiansup. *"Faster elliptic curve arithmetic for double-base chain by reordering sequences of field operations"*. In Proceedings of the International Symposium on Information Theory and its Application — ISITA 2012, pp. 411–415. [PDF]
- Chitchanok Chuengsatiansup, Hiroshi Imai, and Vorapong Suppakitpaisarn. *"Evaluating optimized computation in double-base chain for efficient elliptic curve cryptography"*. In Proceedings of the 15th Japan-Korea Joint Workshop on Algorithms and Computation — WAAC 2012, pp. 56–63. [PDF]

International Conference with Referees (extended abstract review)

- Chitchanok Chuengsatiansup. *"How to write award-winning papers: Mining award-winning paper characteristics"*. In Proceedings of the 4th Thailand-Japan International Academic Conference — TJIA 2011, pp. 111-112. [PDF]

Technical Report

- Chitchanok Chuengsatiansup. *"Efficient atomic block for faster elliptic curve scalar multiplication"*. In a technical report of IEICE, Vol. 112, No. 93, pp. 71-78, June, 2012. [PDF]

Preprints

- Daniel J. Bernstein, Chitchanok Chuengsatiansup, and Tanja Lange. *"Double-base scalar multiplication revisited"*. IACR Cryptology ePrint Archive, 2017. https://eprint.iacr.org/2017/037. [PDF]
- Daniel J. Bernstein, Chitchanok Chuengsatiansup, Tanja Lange, and Christine van Vredendaal. *"NTRU Prime"*. IACR Cryptology ePrint Archive, 2016. https://eprint.iacr.org/2016/461. [PDF]

Theses and Graduation Project

- Chitchanok Chuengsatiansup. *"Optimizing Curve-Based Cryptography"*. Ph.D. Thesis. Eindhoven University of Technology, The Netherlands. 2017. [PDF]
- Chitchanok Chuengsatiansup. *"Improved Elliptic Curve Arithmetic by Reordering Operation Sequences"*. Master's Thesis. The University of Tokyo, Japan. 2013. [PDF]
- Chitchanok Chuengsatiansup. *"How to Write Best Paper: An Approach to Mining Characteristics of Good Papers"*. Graduation Project. Chulalongkorn University, Thailand. 2010.

Invited Talk at International Conference

- *Fast arithmetic on Hessian curves.* Invited talk at the 20th Workshop on Elliptic Curve Cryptography — ECC 2016, September 2016. [Slides]

Presentations at International Conferences with Referees

- *Pairing-friendly twisted Hessian curves.* The 19th International Conference on Cryptology in India — INDOCRYPT 2018, December 2018. [Slides]
- *Kummer strikes back: new DH speed records.* The 20th Annual International Conference on the Theory and Application of Cryptology and Information Security — ASIACRYPT 2014, December 2014. [Slides]
- *Curve41417: Karatsuba revisited.* The 16th Workshop on Cryptographic Hardware and Embedded System — CHES 2014, September 2014. [Slides]
- *Faster elliptic curve arithmetic for double-base chain by reordering sequences of field operations.* The 2012 International Symposium on Information Theory and its Applications — ISITA 2012, October 2012.
- *Evaluating optimized computation in double-base chain for efficient elliptic curve cryptography.* The 15th Japan-Korea Joint Workshop on Algorithms and Computation — WAAC 2012, July 2012.

Presentations at International Conferences with Referees (abstract review)

- *Fast and secure DH implementation.* The 6th International Workshop on Cryptography, Robustness, and Provably Secure Schemes for Female Young Researchers — CrossFyre 2016, July 2016. [Slides]
- *New scalar multiplication speed record.* Student presentation at the 4th International Conference on Cryptology and Information Security in Latin America — Latincrypt 2015, August 2015.
- *Curve41417: fast, highly secure and implementation-friendly curve.* Workshop on Elliptic Curve Cryptography Standards, June 2015.
- *Faster point doubling on twisted Hessian curves.* Student presentation at the 3rd International Conference on Cryptology and Information Security in Latin America — Latincrypt 2014, September 2014. [Slides]
- *How to write award-winning papers: Mining award-winning paper characteristics.* The 4th Thailand-Japan International Academic Conference — TJIA 2011, November 2011.

Presentation at Seminar (abstract review)

- Chitchanok Chuengsatiansup. *"Efficient atomic block for faster elliptic curve scalar multiplication"*. In a technical report of IEICE, Vol. 112, No. 93, pp. 71-78, June, 2012. [PDF]

Invited Presentations at Seminars

- *Fast and secure DH Implementations*. Simula@UiB seminar. Bergen, Norway. (2 October 2018)
- *Optimizing multiplications with vector instruction*. CARAMBA team seminar. Inria Nancy, France. (4 June 2018)
- *Optimizing multiplications with vector instruction*. Project-team Grace seminar. Inria Saclay, France. (19 March 2018)
- *Writing high-speed software using qhasm*. "Jasmine" meeting. Inria Sophia-Antipolis, France. (18 September 2017)
- *Optimizing multiplications with vector instructions*. IMI Crypto seminar. Kyushu University, Japan. (13 February 2017)
- *Optimizing multiplications with vector instructions*. Crypto seminar. ENS de Lyon, France. (16 November 2016)
- *Fast arithmetic on Hessian curves and optimal double-base chains*. Crypto Working Group seminar. Utrecht, The Netherlands. (9 September, 2016)
- *New Diffie–Hellman Speed Records*. Crypto Working Group seminar. Utrecht, The Netherlands. (27 February 2015)

Other Presentations

- *Pond — a non-instant messaging protocol by Adam Langley*. Privacy and surveillance seminar. UC Davis, USA. (4 November 2015)
- *Curve41417: Karatsuba revisited*. Symposium Diamant. The Netherlands. (28 May 2015)
- *Kummer strikes back: new DH speed records*. Ei/PSI seminar. Eindhoven University of Technology. The Netherlands. (7 April 2014)