Chitchanok Chuengsatiansup

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

Informations

Nom : Chuengsatiansup
Prénom : Chitchanok
Lieu de naissance : Bangkok, Thaïlande
Nationalité : Thaïlandaise
Adresse : Laboratoire de l'Informatique du Parallélisme
École Normale Supérieure de Lyon
46 Allée d'Italie 69364 Lyon Cedex 07
France
Adresse électronique : *chitchanok.chuengsatiansup@ens-lyon.fr*
Page web : *https://perso.ens-lyon.fr/chitchanok.chuengsatiansup*

Situation actuelle

J'ai soutenu ma thèse de doctorat le 16 mars 2017. Depuis le 1er mai 2017, je suis chercheuse postdoctorale chez Inria au sein du laboratoire LIP à l'ENS de Lyon, dans le pôle Crypto de l'équipe AriC. En particulier, je travaille sur le projet RISQ : Regroupement de l'industrie française pour la sécurité post-quantique.

Diplômes

2017 **Doctorat en mathématiques et informatique** de l'université technique d'Eindhoven (Technische Universiteit Eindhoven), Pays-Bas
◇ Titre : *"Optimizing Curve-Based Cryptography"*
Traduction : Optimisations de la cryptographie à base de courbes
◇ Soutenue le 16 mars 2017
◇ Avec comme composition du jury :
· Barry Koren, université technique d'Eindhoven, Pays-Bas (président)
· Daniel J. Bernstein, université de l'Illinois à Chicago (University of Illinois at Chicago), États-Unis d'Amérique et université technique d'Eindhoven, Pays-Bas (directeur)
· Tanja Lange, université technique d'Eindhoven, Pays-Bas (directrice)
· Aart Blokhuis, université technique d'Eindhoven, Pays-Bas
· David R. Kohel, université d'Aix-Marseille, France
· Christof Paar, université de la Ruhr à Bochum (Ruhr-Universität Bochum), Allemagne
· Kenneth G. Paterson, Royal Holloway, université de Londres, Royaume-Uni
· Bart Preneel, KU Leuven (Katholieke Universiteit Leuven), Belgique

2013 **Master en informatique** de l'université de Tokyo (*The University of Tokyo*), Japon (mention bien).
◇ Titre de mémoire de master : *"Improved Elliptic Curve Arithmetic by Reordering Operation Sequences"*
Traduction : Améliorer l'arithmétique de courbe elliptique par la réorganisation des déroulements d'operations
◇ Soutenu le 5 avril 2010
◇ Sous la direction du Hiroshi Imai et Vorapong Supakitpaisarn

2010 **Licence en ingénierie informatique** de l'université Chulalongkorn (Chulalongkorn University), Thaïlande (avec mention First Class Honors). Mémoire de fin d'études intitulé *"How to Write Best Paper : An Approach to Mining Characteristics of Good Papers"* (Comment écrire le meilleur article : une façon d'extraire les caractéristiques des bons articles), sous la direction du Boonserm Kijsirikul.

Activités de recherche

2017 – présent	Chercheuse postdoctorale chez Inria au laboratoire LIP de l'ENS de Lyon, membre du pôle Crypto dans l'équipe AriC. Mon activité de recherche porte sur la cryptographie post-quantique.
2013 – 2017	Étudiante en doctorat à l'université technique d'Eindhoven, membre du groupe sur les implantations cryptographiques. Mon thème de recherche était l'optimisation des primitives cryptographiques à base de courbes.
2011 – 2013	Étudiante en master à l'université de Tokyo, membre du laboratoire du professeur Hiroshi Imai. Mon thème de recherche était la cryptographie sur les courbes elliptiques.
2010 – 2011	Étudiante chercheuse à l'université de Tokyo au laboratoire du professeur Hiroshi Imai sur la complexité algorithmique.
2006 – 2010	Étudiante en licence à l'université Chulalongkorn. Membre du club de robotique, j'étais intéressée par les intelligences artificielles permettant aux robots de jouer au football et j'ai participé à des concours nationaux et internationaux de "RoboCup" (abréviation de *Robot Soccer World Cup*).

Centres d'intérêts dans la recherche

- Cryptographie sur les courbes elliptiques et hyperelliptiques
- Cryptographie à base de couplages
- Cryptographie post-quantique
- Réseaux euclidiens
- Attaques par canaux auxiliaires
- Sécurité et vie privée
- Messagerie sécurisée
- Factorisation

Informatique

- Maîrise de Python, Sage, Magma, qhasm et C/C++
- Familière avec le java et l'HTML

Langues

- Thaï (langue maternelle)
- Anglais (courant)
- Japonais (très bon)
- Français (bon)
- Néerlandais (intermédiaire)
- Allemand et Chinois (élémentaires)

Liste des publications et des présentations

Chitchanok Chuengsatiansup

Conférences internationales avec un comité de lecture

- Chitchanok Chuengsatiansup et Chloe Martindale. *"Pairing-friendly twisted Hessian curves"*. Debrup Chakraborty et Tetsu Iwata, editeurs. 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 et Christine van Vredendaal. *"NTRU Prime : reducing attack surface at low cost"*. Carlisle Adams et Jan Camenische, editeurs. 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 et Christine van Vredendaal. *"How to manipulate curve standards : a white paper for the black hat"*. Liqun Chen et Shin'ichiro Matsuo, editeurs. 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 et Tanja Lange. *"Twisted Hessian curves"*. Kristin Lauter et Francisco Rodríguez-Henríquez, editeurs, 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 et Peter Schwabe. *"Kummer strikes back : new DH speed records"*. Palash Sarkar et Tetsu Iwata, editeurs, Advances in Cryptology — ASIACRYPT 2014. Lecture Notes in Computer Science, Vol. 8873, pp. 317–337. Springer (2014). [PDF]
- Daniel J. Bernstein, Chitchanok Chuengsatiansup et Tanja Lange. *"Curve41417 : Karatsuba revisited"*. Lejla Batina et Matthew Robshaw, editeurs, 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 et Peter Schwabe. *"PandA : Pairings and Arithmetic"*. Zhenfu Cao et Fangguo Zhang, editeurs, 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"*. Dans les actes d'International Symposium on Information Theory and its Application — ISITA 2012, pp. 411–415. [PDF]
- Chitchanok Chuengsatiansup, Hiroshi Imai et Vorapong Suppakitpaisarn. *"Evaluating optimized computation in double-base chain for efficient elliptic curve cryptography"*. Dans les actes de la 15th Japan-Korea Joint Workshop on Algorithms and Computation — WAAC 2012, pp. 56–63. [PDF]

Conférences internationales avec sélection sur résumé étendu

- Chitchanok Chuengsatiansup. *"How to write award-winning papers : Mining award-winning paper characteristics"*. Dans les actes de la 4th Thailand-Japan International Academic Conference — TJIA 2011, pp. 111–112. [PDF]

Rapports techniques

· Chitchanok Chuengsatiansup. *"Efficient atomic block for faster elliptic curve scalar multiplication"*. Dans un rapport technique de l'IEICE, Vol. 112, No. 93, pp. 71–78, juin, 2012. [PDF]

Archives ouvertes en ligne

· Daniel J. Bernstein, Chitchanok Chuengsatiansup et 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 et Christine van Vredendaal. *"NTRU Prime"*. IACR Cryptology ePrint Archive, 2016. https://eprint.iacr.org/2016/461. [PDF]

Thèses et mémoires

· Chitchanok Chuengsatiansup. *"Optimizing Curve-Based Cryptography"*. Thèse de doctorat. Université technique d'Eindhoven, Pays-Bas. 2017. [PDF]

· Chitchanok Chuengsatiansup. *"Improved Elliptic Curve Arithmetic by Reordering Operation Sequences"*. Mémoire de master. Université de Tokyo, Japon. 2013. [PDF]

· Chitchanok Chuengsatiansup. *"How to Write Best Paper : An Approach to Mining Characteristics of Good Papers"*. Mémoire de fin d'études (licence). Université Chulalongkorn, Thaïlande. 2010.

Présentations invitées lors de conférences internationales

· *Fast arithmetic on Hessian curves.* Présentation invitée à 20th Workshop on Elliptic Curve Cryptography — ECC 2016, septembre 2016. [Slides]

Présentations lors de conférences internationales avec un comité de lecture

· *Pairing-friendly twisted Hessian curves.* 19th International Conference on Cryptology in India — INDOCRYPT 2018, decembre 2018. [Slides]

· *Kummer strikes back : new DH speed records.* 20th Annual International Conference on the Theory and Application of Cryptology and Information Security — ASIACRYPT 2014, decembre 2014. [Slides]

· *Curve41417 : Karatsuba revisited.* 16th Workshop on Cryptographic Hardware and Embedded System — CHES 2014, septembre 2014. [Slides]

· *Faster elliptic curve arithmetic for double-base chain by reordering sequences of field operations.* 2012 International Symposium on Information Theory and its Applications — ISITA 2012, octobre 2012.

· *Evaluating optimized computation in double-base chain for efficient elliptic curve cryptography.* 15th Japan-Korea Joint Workshop on Algorithms and Computation — WAAC 2012, juillet 2012.

Présentations lors de conférences internationales avec sélection sur résumé

- *Fast and secure DH implementation.* 6th International Workshop on Cryptography, Robustness, and Provably Secure Schemes for Female Young Researchers — CrossFyre 2016, juillet 2016. [Slides]
- *New scalar multiplication speed record.* À la session de présentation des étudiants de la 4th International Conference on Cryptology and Information Security in Latin America — LATINCRYPT 2015, août 2015.
- *Curve41417 : fast, highly secure and implementation-friendly curve.* Workshop on Elliptic Curve Cryptography Standards, juin 2015.
- *Faster point doubling on twisted Hessian curves.* À la session de présentation des étudiants de la 3rd International Conference on Cryptology and Information Security in Latin America — LATINCRYPT 2014, septembre 2014. [Slides]
- *How to write award-winning papers : Mining award-winning paper characteristics.* 4th Thailand-Japan International Academic Conference – TJIA 2011.

Présentations lors de séminaires avec sélection sur lecture

- Chitchanok Chuengsatiansup. *"Efficient atomic block for faster elliptic curve scalar multiplication"*. Dans un rapport technique de l'IEICE, Vol. 112, No. 93, pp. 71–78, juin, 2012. [PDF]

Autres présentations

- *Fast and secure DH implementations*. Présantation invitée au séminaire d'équipe Simula@UiB, Bergen, Norvège. (2 octobre 2018)
- *Optimizing multiplications with vector instructions*. Présantation invitée au séminaire d'équipe CARAMBA, Inria Nancy, France. (4 juin 2018)
- *Optimizing multiplications with vector instructions*. Présantation invitée au séminaire d'équipe GRACE, Inria Saclay, France. (19 mars 2018)
- *Writing high-speed software using qhasm*. Présentation invitée à la réunion « Jasmine » , Inria Sophia-Antipolis, France. (18 septembre 2017)
- *Optimizing multiplications with vector instructions*. Présentation invitée au séminaire IMI Crypto. Kyushu University, Japon. (13 février 2017)
- *Optimizing multiplications with vector instructions*. Présentation invitée au séminaire Crypto. ÉNS de Lyon, France. (16 novembre 2016)
- *Fast arithmetic on Hessian curves and optimal double-base chains*. Réunion de Crypto Working Group. Utrecht, Pays-Bas. (9 septembre, 2016)
- *Pond — a non-instant messaging protocol by Adam Langley*. Séminaire la vie privée et la surveillance. UC Davis, USA. (4 novembre 2015)
- *Curve41417 : Karatsuba revisited*. Symposium Diamant. Veenenaal, Pays-Bas. (28 mai 2015)
- *New Diffie–Hellman Speed Records*. Réunion de Crypto Working Group. Utrecht, Pays-Bas. (27 février 2015)
- *Kummer strikes back : new DH speed records*. Séminaire Ei/PSI. Université technique d'Eindhoven, Pays-Bas. (7 avril 2014)