Tarik Kaced

Curriculum vitæ

Né le 2 mars 1986 — Metz, Moselle (57)
Nationalité française
Permis B

Contact Personnel

16 Allée des marguerites
57420 Pournoy-La-Chétive

Tél.: 06 17 40 92 38
Mel: tarik.kaced@ens-lyon.org
Site web: http://www.chezlefab.net/~tkaced/

Position actuelle: Néant

Intérêts scientifiques

Aspects théoriques de la théorie de l'information, inégalités d'information, sécurité (in)conditionelle, partage de secret, complexité de Kolmogorov et calculabilité, théorie des codes et cryptographie, complexité de communication, liens avec la théorie des graphes et la théorie des matroïdes, les sous-shifts,

Formation

mars 2016 – sept. 2016 ***Khôlleur*** de mathématiques en classe préparatoire ECS au lycée Saint-Louis à Paris

avril 2015 – fev. 2016 ***Post-doctorant*** au Laboratoire d'Algorithmique, Complexité et Logique, UPEC, (Université Paris-Est Créteil).

2013–2015 ***Post-doctorant*** à l'Institute of Network Coding, CUHK (The Chinese University of Hong Kong).

2011–2012 ***Allocataire de recherche moniteur***, doctorant en 3^e année au LIRMM, (Laboratoire d'Informatique de Robotique et de Microélectronique de Montpellier), Université de Montpellier 2. Sous la direction d'Andrei Romashchenko et Alexander Shen.
Intitulé de la thèse : Partage de secret et théorie algorithmique de l'information.

- definition et étude des schémas de partage de secret presque parfaits.
- découverte des inégalités *essentiellement* conditionelles pour l'entropie de Shannon
- définition des versions Kolmogorovienne des deux notions précédentes
- preuve d'équivalence de deux techniques da dérivation d'inégalités de type non-Shannon.

2009–2011 ***Doctorant*** en Informatique Fondamentale à l'Université de Provence, Marseille. Centre de Mathématique et d'informatique (CMI) au sein du LIF, Équipe Escape.

2007–2009 ***Master recherche*** d'informatique (PENSUNS), parcours Systèmes Complexes, Université de Nice Sophia-Antipolis, , antenne de l'ÉNS LYON, Mention Très Bien.
Matières principales : Complexité de Kolmogorov, Automates cellulaires, Lambda-calcul et Catégories, Nombres Jeux et Stratégies, Cryptographie et Sécurité

2006–2007 ***Licence*** en Informatique Fondamentale, École Normale Supérieure de Lyon.
Matières principales : Fondements de l'Informatique, Programmation, Architecture Système et Réseaux, Algorithmique, Coq
Récipiendaire d'une bourse de 3 ans du Conseil Général des Alpes Maritimes en partenariat avec l'ENS Lyon et l'UNSA.

2003–2006 ***CPGE***, Classes Préparatoires aux grandes Écoles, Lycée Fabert, Metz (57).

Stages de recherche

2009 (Février–Août) ***Stage de recherche*** sous la direction de Bruno Durand, Andrei Romashchenko et Alexander Shen. Théorie du partage de secret et complexité de Kolmogorov, CMI - LIF, Marseille

2008 (Juin–Août) ***Stage de recherche*** sous la direction de Wolfgang Merkle, Complexité de Kolmogorov, Universität Heidelberg, Allemagne.

2007 (Juin–Juillet) ***Stage de recherche*** sous la direction de Judicaël Courant et Yassine Lakhnech, Preuve de protocoles cryptographiques pour la redistribution dans le partage de secret. VERIMAG, Grenoble

Enseignement (216h éq.TD.)

2016 ***Khôlleur*** au Lycée Saint-Louis, (22h)

2015 ***Vacataire*** à l'UPEC (Paris 12), (90h)

2013 ***Mini-cours invité*** à l'Institute of Network Coding, (15h)

2011 ***Moniteur*** de l'Université de Montpellier 2, DCCE, (64h), mission complémentaire d'enseignement.

2008 ***Vacataire*** de l'Université de Nice Sophia-Antipolis (20h)

Détail

2016 Khôlleur de Mathématiques en ECS 1ère année pour le cours de Boyer, 22h
2015–2016 TP Python 3 en M1 Info, cours de Pascal Vanier, 12h
2015–2016 TD de Structures de Données en L2 Info, cours de Serghei Verlan, 9h
2015–2016 TD d'Initiation aux bases de données en L2 Info, cours de Antoine Spicher, 18h
2015–2016 TD d'Initiation à l'algorithmique en L1 Info/SPI/SVT, cours de Catalin Dima, 21h
2015–2016 TD de Programmation en L1 Info et SPI, cours de Catalin Dima, 22.5h
2013 Mini-cours invité sur la Complexité de Kolmogorov, destiné aux chercheurs et étudiants (15h)
2011-2012 TP Algorithmes de graphes en L3 Info (18h), `GLIN501` cours de Stéphane Bessy
2011-2012 TP Analyse d'algorithmes en L3 Info (18h), `GLIN503` cours d'Hervé Dicky et de Bruno Durand
2011-2012 TP C2I en L1 (27h), `GLIN102` cours de Sylvain Daudé et Michelle Joab
2011-2012 TD Théorie de l'information en M1 Info (3h), cours de Gregory Lafitte
2011-2012 TD Algorithmes de graphe en L3 Info (3h), `GLIN501` cours de Stéphane Bessy
2008–2009 Tutorat OFI en L2 Math-Info (20h), cours d'outils formels pour l'informatique à l'Université de Nice Sophia-Antipolis.

Activités

Relectures:

conférence `UCNC` 2012–2014, `ISIT` 2012-2015, `NETCOD2014`, `CyberC2015`
journal Designs, Codes and Crypto., Trans. on Inf. Theory, Trans. on Communications, Theory of Comp. Sys., ENTROPY, Kybernetica
2014 Co-encadrement avec Sidarth Jaggi d'un groupe d'étudiants sur un projet qui a donné lieu à une publication.
2013-2014 Co-organisation avec C. Chung et K. Shum d'un groupe de travail sur les matroïdes
2011–2012 Co-responsable avec F. Givors du Groupe de travail de l'équipe Escape au LIRMM
2011–2012 Formation C2I niveaux 1 et 2, DCCE (24h)
2010–2011 Responsable du Groupe de travail de l'équipe Escape au LIF

Publications & présentations

7 publications en conférences avec comité de lecture

2015 avec C. Chan, A. Al-Bashabsheh, J.B. Ebrahimi, S. Kadhe, T .Liu, A. Sprintson, M. Yan, Q. Zhou, ***Successive Omniscience***, `NetCod`, IEEE
2014 avec O. Farràs, T. Hansen, C. Padró, ***Optimal Non-Perfect Uniform Secret Sharing Schemes***, CRYPTO 2014, ePrint
2014 avec T. Li, C.L. Chan, W. Huang, S. Jaggi, ***Group Testing avec Prior Statistics***, ISIT 2014, `arXiv:1401.3667`

2013 ***Equivalence of Two Proof Techniques for Non-Shannon-type Inequalities***, IEEE Proceedings ISIT 2011, Istanbul, Turkey, pp. 236-240, arXiv:1302.2994

2012 avec A. Romashchenko, ***On the Non-robustness of Essentially Conditional Information Inequalities***, ITW 2012, arXiv:1207.5458

2011 avec A. Romashchenko, ***On Essentially Conditional Information Inequalities***, ISIT 2011, St. Petersburg, Russia, pp. 1935-1939, arXiv:1103.2545

2011 ***Almost Perfect Secret Sharing***, ISIT 2011, St. Petersburg, Russia, pp. 1603-1607, arXiv:1103.2544

5 publications dans des journaux

2016 avec C. Chan, A. Al-Bashabsheh, T. Liu, Qiaoqiao Zhou, ***Info-Clustering: A Mathematical Theory for Data Clustering***, accepté, IEEE Transactions on Molecular, Biological, and Multi-Scale Communications.

2016 avec O. Farràs, T. Hansen, C. Padró, ***On the Information Ratio of Non-Perfect Secret Sharing Schemes***, Algorithmica, ePrint

2015 avec C. Chan, A. Al-Bashabsheh, J. Ebrahimid, T. Liu, ***Multivariate Mutual Information Inspired by Secret Key Agreement***, *IEEE Trans. on Information Theory*, vol.103, no.10, IEEE

2012 avec A. Romashchenko, ***Conditional Information Inequalities for Entropic and Almost Entropic Points***, *IEEE Trans. on Information Theory*, vol. 59, no. 11

2012 ***Quasi-perfect secret sharing***, accepté, Information and Computation.

3 articles soumis / en préparation

2017 ***The Entropy Region is not Closed Under Duality***, journal, soumis, arXiv:1611.04109

2015 avec Qi Chen, ***New Facets of*** Γ_3^*, en préparation

2015 avec A.Romashchenko, N. Vereshchagin, ***Conditional Information Inequalities and Combinatorial Applications***, journal, soumis, arXiv:1501.04867

Communications orales

avr. 2017 Séminaire du LIFO: TBA

avr. 2016 ***(Invité)*** BarcelonaTech Séminaire MAK: *Dual Information Inequalities*

mar. 2016 ***(Invité)*** Nexus of Information and Computation Theories: *Dual Information Inequalities*

avr. 2015 Journées Calculabilités: *Dual Information Inequalities*

mar. 2015 Séminaire LORIA: *Optimal Non-perfect Uniform Secret Sharing Schemes*

fév. 2015 ***(Invité)*** ITA: *Conditional Information Inequalities and Biclique Coverings*

janv. 2015 ITCOM: *New Constrained Information Inequalities and Possible Applications*

mai 2014 Séminaire CANDOIT: *Optimal Non-Perfect Secret-Sharing*

juil. 2013 ISIT: *Equivalence of Two Proof Techniques for Non-Shannon-type Inequalities*

mai 2013 ***(Invité)*** Mathematics of Information Theoretic Crypto: *Essentially Conditional Information Inequalities Might Help*, Leiden

avril 2013 ***(Invité)*** Workshop on Entropy and Information Inequalities, *Essentially Conditional Information Inequalities*

fév. 2013 Séminaire INC, *Secret Sharing and Information Inequalities*

mars 2012 Journées Calculabilités, *Essentially conditional information inequalities*, Paris.

août 2011 Conférence `ISIT 2011`, *Almost perfect secret sharing*, Saint-Petersbourg.

mai 2011 Groupe de travail Escape (LIF), *(Un)constrained Linear Information Inequalities*, Marseille.

mai 2010 Groupe de travail Escape (LIF), *Exposé des travaux*, Marseille.

avril 2010 EJC IM 2010, *Comment partager un secret*, Chambéry.

avril 2010 FRAC de printemps, *Secret Sharing*, Caen.

juil. 2008 Oberseminar Universität Heidelberg, *Secret Sharing and Provable Security*, Heidelberg (Allemagne).

Bourses & financements

2013–2015 Bourse post-doctorale de 2 ans à l'Institute of Network Coding

2006–2009 Récipendiaire d'une bourse de 3 ans de l'ÉNS de Lyon et du conseil régional de Alpes-Maritimes

2008 Financement de l'Université de Floride pour l'école d'été "Algorithmic Randomness" à Gainesville

2007 Financement de l'ÉNS pour ESSLLI 2007 à Dublin