CONSEILLER SCIENTIFIQUE

PHILIPPE ELBAZ-VINCENT

Professeur
Univ. Grenoble Alpes

Philippe Elbaz-Vincent est professeur des universités en Mathématiques à l'Université Grenoble Alpes depuis 2007. Ses domaines de recherche sont la théorie des nombres, en particulier la géométrie des nombres et la cohomologie des groupes arithmétiques, les polylogarithmes et leurs interactions avec la théorie de l'information, la cryptologie et la cybersécurité. Il a été Marie Curie fellow de l'UE en 1998-1999, et a été chercheur invité à l'IHÉS, au MPI für Mathematik (Bonn), à l'EPFL et au Haussdorf Institute für Mathematik (Bonn). Il a encadré plus de 20 alumnis (doctorants, post-doctorants et collaborateurs scientifiques) et a été partenaire ou (co)responsable d'une vingtaine de projets de recherche (e.g., ANR, FUI, PIA). Il est actuellement directeur du Grenoble Alpes Cybersecurity Institute de l'IDEX Univ. Grenoble Alpes.

Autres responsabilités exercées

- Responsable pédagogique de la filière en apprentissage et alternance «Cybersécurité et Informatique légale» du Master d'Informatique de l'UGA
- Membre du Comité de coordination scientifique de l'Institut Carnot LSI

Principales publications

- **Elbaz-Vincent Ph., Müller-Stach S. (2002) ;** Milnor K-theory of rings, higher Chow groups and applications, Inventiones Math. Volume 148 Issue 1 (2002) , 177-206.
- **Elbaz-Vincent Ph., Gangl H. (avec un appendice de M. Kontsevich) (2002);** On Poly(ana)logs I, Compositio Mathematica 130 (2) : 161-214, (2002).
- **Elbaz-Vincent Ph., Gangl H., Soulé C. (2013) ;** Perfect forms, K-theory and the cohomology of modular groups, , Advances in Mathematics 245 (2013) 587-624.
- **Elbaz-Vincent Ph. (2004);** A Short Introduction to Higher Chow groups, Proceedings of the Lecture Summer School, Grenoble 2001, "Transcendental Aspects of Algebraic Cycles" edited by S. Müller-Stach and C. Peters. Lecture Notes 313 of the LMS, Cambridge University Press (2004), 171-196.
- **Sarr A. P., Elbaz–Vincent Ph. (2012):** A Complementary Analysis of the (s)YZ and DIKE Protocols, AfricaCrypt 2012, Mitrokotsa, Aikaterini ; Vaudenay, Serge (Eds.), Springer LNCS 7374 (2012), 203-220.
- **Soucarros M., Clediere J., Dumas C. and Elbaz-Vincent Ph. (2013):** Methodology for the Fault Analysis and Evaluation of True Random Number Generators, HAL : hal-00678001, Journal of Electronic Testing June 2013, Volume 29, Issue 3, 367-381 (double colonnes)
- **Sarr A., Elbaz-Vincent Ph. and J.-C. Bajard (2010);** A New Security Model for Authenticated Key Agreement, Security and Cryptography for Networks 7th International Conference, SCN2010, Amalfi, Italy, September 13-15, 2010. Garay et Brisco (Eds), Lecture Notes in Computer Science Volume 6280, 2010, DOI : 10.1007/978-3-642-15317-4, 219-234.
- **Elbaz-Vincent P., Gangl H. (2015);** Finite Polylogarithms, Their Multiple Analogues and the Shannon Entropy. In: Nielsen F., Barbaresco F. (eds) Geometric Science of Information. GSI 2015. Lecture Notes in Computer Science, vol 9389. Springer, Cham
- **Sarr A.P., Elbaz–Vincent P. (2016);** On the Security of the (F)HMQV Protocol. In: Pointcheval D., Nitaj A., Rachidi T. (eds) Progress in Cryptology – AFRICACRYPT 2016. AFRICACRYPT 2016. Lecture Notes in Computer Science, vol 9646. Springer, Cham
- **Tofighi-Shirazi R., Christofi M., Elbaz-Vincent Ph. and Le, T.-ha (2018);** DoSE: Deobfuscation Based on Semantic Equivalence, In Proceedings of the 8th Software Security, Protection, and Reverse Engineering Workshop (SSPREW-8). ACM, New York, NY, USA,1-12. DOI: https://doi.org/10.1145/3289239.3289243