Computational aspects of class group actions and applications to post-quantum cryptography

Houben, M.R.

Curriculum Vitae

Marc Houben was born on 16 March 1995 in Utrecht, The Netherlands. He grew up in Houten, where he went to high school College de Heemlanden from 2007, obtaining his diploma in 2013.

After that, he studied at Utrecht University, where in 2016 he obtained bachelor degrees *cum laude* in both Mathematics and Physics. His bachelor's thesis on "Congruences for coefficients of power series expansions of rational functions" was written under supervision of prof. dr. Frits Beukers. He continued studying Mathematics at Utrecht University, obtaining a master's degree *cum laude* in 2018. His master's thesis on "Dynamics on algebraic groups" was written under supervision of prof. dr. Gunther Cornelissen.

In October 2018, Marc started a joint PhD in Mathematics between KU Leuven and Leiden University under supervision of dr. Wouter Castryck and dr. Marco Streng. In November 2019, he began a PhD Fellowship fundamental research from Research Foundation – Flanders (FWO). Since October 2021, Marc is a visitor at the Computer Security and Industrial Cryptography (COSIC) group at KU Leuven.

List of Publications

This thesis is based on the following published papers.

[1] **Weak instances of class group action based cryptography via self-pairings.**
Wouter Castryck, Marc Houben, Simon-Philipp Merz, Marzio Mula, Sam van Buuren, and Frederik Vercauteren.
CRYPTO 2023.

[2] **Horizontal racewalking using radical isogenies.**
Wouter Castryck, Thomas Decru, Marc Houben, and Frederik Vercauteren.
ASIACRYPT 2022.

[3] **On the decisional Diffie–Hellman problem for class group actions on oriented elliptic curves**.
Wouter Castryck, Marc Houben, Frederik Vercauteren, and Benjamin Wesolowski.
ANTS XV. In Res. Number Theory 8.4, Paper No. 99, 18. 2022.

[4] **Generalized class polynomials.**
Marc Houben and Marco Streng.
ANTS XV. In Res. Number Theory 8.4, Paper No. 103, 26. 2022.

The author of the thesis has additionally published the following papers that are not included in the thesis.

[5] **Dynamically affine maps in positive characteristic.**
Jakub Byszewski, Gunther Cornelissen, and Marc Houben, with Appendix B by the authors and Lois van der Meijden.
Contemporary Mathematics 744. pp. 125–156, 2020.

[6] **Gauss congruences for rational functions in several variables.**
Frits Beukers, Armin Straub, and Marc Houben.
Acta Arithmetica 184.4, pp. 341-362, 2018.