GOPPA–LIKE AG CODES FROM $C_{a,b}$ CURVES AND THEIR BEHAVIOUR UNDER SQUARING THEIR DUAL

SABIRA EL KHALFAOUI, MATHIEU LHOTEL, AND JADE NARDI

Abstract. In this paper, we introduce a family of codes that can be used in a McEliece cryptosystem, called *Goppa–like AG codes*. These codes generalize classical Goppa codes and can be constructed from any curve of genus $\mathfrak{g} \geq 0$. Focusing on codes from $C_{a,b}$ curves, we study the behaviour of the dimension of the square of their dual to determine their resistance to distinguisher attacks similar to the one for alternant and Goppa codes developed by Mora and Tillich [**?**]. We also propose numerical experiments to measure how sharp is our bound.

References

Univ Rennes, IRMAR - UMR 6625, F-35000 Rennes, France
Email address: sabira.elkhalfaoui@univ-rennes1.fr

Laboratoire de Mathématiques de Besançon, UMR 6623 CNRS Université de Bourgogne Franche-Comté, France
Email address: mathieu.lhotel@univ-fcomte.fr

Univ Rennes, CNRS, IRMAR - UMR 6625, F-35000 Rennes, France
Email address: jade.nardi@univ-rennes1.fr

Date: May 15, 2023.
2020 *Mathematics Subject Classification.* 11T71, 14G50, 14H05, 11G20.
Key words and phrases. AG codes, Subfield subcodes, $C_{a,b}$ curves, Goppa–like AG codes, Trace codes, Schur product.