A Secure Implementation of a Goppa Decoder

Pierre-Louis Cayrel[1], Viktor Fischer[1], **Tania RICHMOND**[1], Pascal Véron[2]

[1] Laboratoire Hubert Curien,
Rue du Prof. Benoit Lauras, 18,
42000, Saint-Etienne, France.
{pierre.louis.cayrel,fischer,tania.richmond}@univ-st-etienne.fr
[2] Institut de Mathématiques
B.P. 20132,
83957, La Garde, France.
veron@univ-tln.fr

Abstract

The irreducible binary Goppa codes are widely used in code-based cryptography, like in the McEliece cryptosystem. The aim of this work is to design an efficient and secure hardware implementation of a Goppa decoder. Patterson proposed in 1975 an algorithm able to efficiently decode those codes. We will show how to adapt this algorithm to obtain a "leakage resistant" variant.