

Abstract. We introduce two new left-to-right integer recodings which can be used to perform scalar multiplication with a fixed sequence of operations. These recodings make it possible to have a simple power analysis resistant implementation of a group-based cryptosystem without using unified formulas or introducing dummy operations. This approach is very useful for groups in which the doubling step are less expensive than the addition step, for example with hyperelliptic curves over binary fields or elliptic curves with mixed coordinates.