Abstract

One of the major threats to the security of cryptosystems nowadays is the information leaked through side channels. For instance, power analysis attacks have been successfully mounted on cryptosystems embedded into small devices such as smart cards. In the recent past, several DPA countermeasures have been proposed. Among these, two countermeasures, one proposed by Oswald and Aigner in [27] and the other by Ha and Moon in [11], are based on inserting random decisions throughout the execution of algorithms that are used to compute the elliptic curve (EC) scalar multiplication using a redundant binary signed digit (BSD) representaiton of the scalar. One important advantage of these two algorithms is that a recoded scalar does not need to be stored. In this report, we investigate the effect of these countermeasures on the execution paths taken by the scalar multiplication algorithms and their average computational complexity. This enables us to present a comparison of these two countermeasures.