Abstract

So-called nonadjacent representations are commonly used in elliptic curve cryptography to facilitate computing a scalar multiple of a point on an elliptic curve. A nonadjacent representation having few non-zero coefficients would further speed up the computations. However, any attempt to use these techniques must also consider the impact on the security of the cryptosystem. The security is studied by examining a related discrete logarithm problem, the topic of this paper. We describe an algorithm to solve the relevant discrete logarithm problem in time that is approximately the square root of the search space. This algorithm is of the familiar "baby-step giant-step" type. In developing our algorithm we use two tools of independent interest; namely, a combinatorial set system called a "splitting system" and a new type of combinatorial Gray code.