Okeya, Katsuyuki; Sakurai, Kouichi

Fast multi-scalar multiplication methods on elliptic curves with precomputation strategy using Montgomery trick. (English) [Zbl 1028.94025]


Summary: Our development of efficient methods for the precomputation of multi-scalar multiplication for elliptic curve cryptosystems (ECCs) is presented. Multi-scalar multiplication is required in many forms of ECC, including schemes for the verification of ECDSA signatures. The simultaneous method is one known method for fast multi-scalar multiplication. The method has two stages: a precomputation stage and an evaluation stage. Points for use in the evaluation stage are computed in the precomputation stage. The actual multi-scalar multiplication is carried out on the basis of the precomputed points in the evaluation stage. In the evaluation stage of the simultaneous method, we are able to quickly compute the points of the multi-scalar multiple because few additions are required. On the other hand, if we use a large window width, we have to compute an enormous number of points in the precomputation stage. Hence, we have to compute an abundance of inversions, which carries a high computational cost. The result is that a large amount of time is required by the precomputation stage. This is the well-known draw-back of the simultaneous method. In our proposed method, we apply the Montgomery trick to reduce the number of inversions required with a width window from $O(2^{2w})$ to $O(w)$. In addition, our proposed method computes $uP$ and $vQ$ for any $u, v$, then compute $uP + vQ$, where $P, Q$ are elliptic points. This procedure enables us to remove points that will not be used later from the process of precomputation. Without our proposed method, an algorithm to compute precomputation table would have to be changed dependently on unused points. Compared with the method without the Montgomery trick, our proposed method is 3.6 times faster than the conventional simultaneous method, i.e., than in the absence of the Montgomery trick. Moreover, the optimal window width for our proposed method is 3, whereas the corresponding width for conventional simultaneous methods is 2.

For the entire collection see [Zbl 1007.00053].

MSC:

94A60 Cryptography
14G50 Applications to coding theory and cryptography of arithmetic geometry
68M07 Mathematical problems of computer architecture
68W40 Analysis of algorithms

Keywords:
elliptic curve cryptography; multi-scalar multiplication; precomputation; Montgomery trick; simultaneous method

Full Text: Link