Stochastic heuristic approach to addition chain problem in PKC for efficiency and security effectiveness

ABSTRACT

This paper shows that stochastic heuristic approach for implicitly solving addition chain problem (ACP) in public-key cryptosystem (PKC) enhances the efficiency of the PKC and improves the security by blinding the multiplications/squaring operations involved against side-channel attack (SCA). We show that while the current practical heuristic approaches being deterministic expose the fixed pattern of the operations, using stochastic method blinds the pattern by being unpredictable and generating diffident pattern of operation for the same exponent at a different time. Thus, if the addition chain (AC) is generated implicitly every time the exponentiation operation is being made, needless for such approaches as padding by insertion of dummy operations and the operation is still totally secured against the SCA. Furthermore, we also show that the stochastic approaches, when carefully designed, further reduces the length of the operation than state-of-the-art practical methods for improving the efficiency. We demonstrated our investigation by implementing RSA cryptosystem using the stochastic approach and the results benchmarked with the existing current methods.

Keyword: RSA; Public-key cryptography; Modular exponentiation