Elliptic Curve Discrete Logarithm Encryption Schemes:

Accelerating the Computations and the Security Considerations.

Ruma Kareem K. Ajeena
Mathematics Department, Education College for Pure Sciences,
University of Babylon, Babil city, 10052, Iraq.
ruma.usm@gmail.com

Abstract. A rich and beautiful history of elliptic curves make them as a fundamental tool to study by several mathematicians for over a hundred years. In 1985, Miller and Koblitz suggested the usage of the elliptic curves in designing the public key cryptosystems. Several researches have been published on the efficient implementation and security of elliptic curve cryptography (ECC). ECCs consider as a more efficient public key cryptosystems because they have smaller key sizes, faster encryption, better security and more efficient implementations for the same security level in comparison with other public cryptosystems say RSA. The efficiency of the elliptic curve cryptosystems depend on the efficient computations of the scalar multiplication *kP* on elliptic curve *E* defined over a prime field F_p. An elliptic scalar multiplication is a core operation in elliptic curve cryptosystem (ECC). It is not only the main computational operation in ECC, but also forms a central time-consuming process. The efficient performances of scalar multiplication directly determines ECC performance. On the other hand, the security of the ECCs depends on the hard mathematical problem which is called the elliptic curve discrete logarithm problem (ECDLP). On the ECDLP modulo p, further of the public key encryption schemes have been constructed. Elliptic curve Diffie–Hellman (ECDH) key agreement protocol, elliptic ElGamal public key cryptosystem (EEPKC) and elliptic curve digital signature algorithm (ECDSA) are examples of the public key encryption schemes depending on ECDLP.

This work proposes the modifications of the ECDH, EEPKC and ECDSA through computing an elliptic curve scalar multiplication by employing the integer sub-decomposition (ISD) method instead of using doubling and addition points on E over a prime field F_p. The modified methods, namely the ECDH-ISD, EEPKC-ISD and ECDSA-ISD algorithms, are benefited from the fast computations in the ISD method, which is depended on the sub-decomposition of the scalars *k* in scalar multiplications *kP*. The ECDH-ISD, EEPKC-ISD and ECDSA-ISD methods also depend on speeding the computations of the efficiently computable endomorphisms ψ of elliptic curve E over finite fields in ISD method. On the other hand, the security level of the modified ECDH-ISD, EEPKC-ISD and ECDSA-ISD algorithms are determined based on the hardness of solving the ECDLP from its sub-decomposition. So, for these reasons, the modified ECDH-ISD, EEPKC-ISD and ECDSA-ISD algorithms are considered as more fast and secure to resist the ECDLP attacks. Therefore, they are more efficient in compared to ECDH, EEPKC and ECDSA respectively.

Keywords: ECCs, scalar multiplication, ECDLP , ISD method, ECDH, EEPKC, ECDSA.