CONCLUSION AND FUTURE WORK

The thesis presented advancement of the Discrete Logarithmic Problem (DLP) in the following four primitives of cryptography such as: Elliptic Curve Cryptography (ECC), Twisted Edwards Curves, Noncommutative Cryptography (NCC), multilayer key generation for ECC using signcryption, and proxy re-cryptographic approach in correlation with the signcryption. All these primitives, on behalf of the research gap, have formulated into five objectives. The chapter 1 presents an introduction related to all the five objectives. The respective objectives are concluded as below from (i) to (v):

(i) The first objective, chapter 2, pertains to Radix-16 scalar multiplication without pre-computation for ECC as a regular scheme. This radix shows the more appropriateness for reduced instruction set computing (RISC) architecture devices and is particular suitable for low memory devices. The proposed approach is against the attacks from simple side channel attacks and safe-error fault attacks. The approach is considered to be on high demanding with respect to software and hardware performance considerations. The major distinction is its computing speed 6.25% faster than recently proposed Radix-8 scalar multiplication technique without pre-computation. A hardware schematic is presented that can be applied for any applications. In reference to this the performance also gets improved by 8.33% on the proposed radix.

(ii) The second objective, chapter 3, contains the architecture of prime Edward curves and extended Twisted Edwards curves on 4 and 8-processors to solve the Edwards curves and extended Twisted Edwards curves problem for scalar multiplication on reduced computation cost with significant improvements. The comparative reduction cost on the 4-processors is \(2M + 1S + 1D + 3A\) to \(2M + 1S + 1D + 2A\) and on the 8-processors is \(2M + 3A\) to \(2M + 2A\). This claims a significant improvement having gained the computational efficiency for Elliptic Curve Cryptography (ECC). The ECC is justifying the security strength and effectiveness on the shorter key lengths.

(iii) The third objective, chapter 4, pertains on Noncommutative Cryptography (NCC), which is a fascinating area on security and performance enhancement. A proposed scheme is based on the extra special group for finding the solution of an open problem for the most appropriate
Noncommutative platform. Regarding this the minimum group of the dihedral order, changes from $D_3$ to $D_4$, enhances the search space and makes the proposal stronger than all the previously predicted group. The basis of this group is established on the Hidden subgroup or subfield problem (HSP), where Conjugacy search problem (CSP) is likely to be intractable. The working principle is based on the random polynomials chosen by the communicating parties to secure key-exchange, encryption-decryption and authentication schemes on NCC. Further, this is enhanced from the general group elements to equivalent ring elements, known by the monomials generations for the cryptographic schemes. The group of orders is more challenging to attack like length based automorphism and brute-force attacks. It provides a high level of safety measures.

(iv) The fourth objective, chapter 5, is based on the secure composition derivation approach for multilayered consensus on key generation with significant improvement using the signcryption primitive. The results for ECC and multilayer consensus key generation approach tested on SPAN and Automated Validation of Internet Security Protocol Architecture (AVISAP) tool. It is showing in information security the proposed approach makes scientifically strong security mechanisms in applied cryptography.

(v) The fifth objective, a combined effort as represented in chapter 6-7, covers a probably secure and efficient approach with regards to the trust problem for third party, who is not directly involved ‘called proxy’, can be solved using signcryption re-cryptographic approach. In modern era of cryptography, this is one of the new diverse trends and motivating issues. Research interest focuses on situations under a cryptographic key management by a semi-trusted proxy with special information where data encrypted under one cryptographic key need to be re-encrypted. In correlation to the same, the presented work is a motivation for the new direction of cryptograph using signcryption. Further, same work is simulated on AVISPA/SPAN, using the automated formal verification tool. An application scenario for Telemedicine has also been simulated on above tool.

In addition, in regards to the proposed work, still future works are: (i) To give a more efficient technique than the radix-16 scalar multiplication without Precomputation. (ii) To make a more feasible solution for Edward’s and twisted Edward’s curve is a demanding issue. (iii) For noncommutative platform to give the solution for open problem. (iv) To give a more insight in
collection of the collect the long-term schemes using proxy re-cryptography applications that best evaluate their suitability for various applications at a single location (v) The approach for modern cryptography with security requirements is arisen in different distributed environments as the attacks may come either from internal or external objects, (v) Using the standard model of proxy re-cryptography make it to more efficient and collusion-resistant to till date, and etc.