CHAPTER 6

CONCLUSION AND FUTURE WORK

6.1 CONCLUSION

The security architectures for Software defined radio which supports authentication, integrity and encryption has been developed and implemented in this research work. Literatures available on security issues and hardware implementation of various cryptographic algorithms were considered for developing the architectures for software defined radio.

The developed architectures for data integrity, authentication and encryption verified with the test vectors for the performance analysis. The hardware utilization, throughput analysis, power consumption and frequency of operation are analyzed to examine the performance of developed architectures.

The architecture developed for data integrity was designed by combining MD5 algorithm and proposed SHA-192 algorithms. The architecture is reconfigurable in the sense it operates in two different modes i.e. one time it uses MD5 and next time it uses SHA-192 hash functions. The developed architecture occupies less area and it also consumes less power than the existing individual architectures. The synthesis result analysis shows that the area occupied by the proposed architecture is very less by 50% to 2600% of area occupied by conventional architectures. The power
consumption of proposed architecture is reduced by 75% than the existing designs.

For entity authentication and key agreement in SDR, the research focused on design of hardware architecture for public key protocols based on modular exponentiation. Novel reconfigurable authentication architecture was developed using RSA and DH algorithms. The RSA algorithm is implemented using division, extended Euclid algorithm and Montgomery exponentiation. Same Montgomery exponentiation architecture is utilized for developing DH algorithm. This eliminates the area overhead and reduces power consumption of authentication unit. The synthesis results are compared with earlier implementations. Modulo inversion is implemented hardware using Extended Euclidean Algorithm.

Design and implementation of hardware architecture of AES was one of the main theme in the research work reported in this thesis. Algorithm implemented in hardware with reconfigurable key size to implement all the three keys, 128-bit, 192- bits and 256-bit keys in the same hardware. Various architecture were developed for providing different combination of performance and power consumption. In all the design a good balance was maintained between quantities, which make it well suited for embedded wireless devices. This makes the entire process of AES algorithm and makes it more complex and provides further resistance against attacks. The developed architecture is found to have excellent throughput rate of 16.6 Gbps with previous implementations. The area occupied is also significantly less.

6.2 SCOPE FOR FUTURE WORK

This research effort creates several opportunities for future investigations. The major future investigations to be
For authentication and key agreement in SDR the research focuses on the design hardware architecture for public key protocols based on modular exponentiation. In future decreasing the exponentiation performance the amount of computation resource can be reduced which improves the efficiency.

The symmetric key algorithms can also be used for authentication and key agreement, can be implemented with significantly low resources and imply high performance.

Numerous attacks against information system are currently performed e.g. through social engineering which can by pass any cryptographic protection mechanism. Therefore as commonly stated it must be remembered that security is not a product that can be developed and sold. It is a continuing process that requires constant research, development and management.