CHAPTER 5

CONCLUSION

5.1 FINAL OBSERVATIONS

The Elliptic Curve Cryptography implemented in Verilog HDL provides a highly efficient encryption algorithm compared to existing algorithms such as RSA and DSA. Further it is achieved an equivalent strength with a key of lesser number of bits (150 – 200 bits). However, selecting a suitable curve and finite field are crucial for ECC security. In this work a method for implementing elliptic curve cryptography using verilog HDL has been provided. Since the proposed hardware implementation of ECC algorithm has shorter key length, shorter parameters and shorter calculation time it proves to be efficient than other cryptographic algorithms. The simulation results provide further proof of the efficiency of the algorithm. The synthesis report gives the details upto the gate level for the logic blocks along with timing summary. The Place and route mapping for the system is achieved. Hardware architectures are much more dependant on the varying bit size than a software implementation.

This method is useful in real-world applications especially in cases wherein large volumes of sensitive data need to be transmitted secretly over public communications channels such as Internet. Experimental results show that the proposed hardware model is more secure compared to the software approach. This approach will be a great building block for strong security applications in areas where high security, high speed and compactness are required. The smaller key size facilitates faster computations, reductions in
processing power, storage space and bandwidth. Various applications include smart cards, pagers, PDAs and cellular phones.

### 5.2 FUTURE SCOPE

For ECC, as the domain parameters (and therefore the abstract group structure) are public, it is straightforward to add a new condition to the exclude list in the domain parameter validation routine. The updated domain parameter validation routine can be run by a user or by a third party (such as a CA) on behalf of the user. One can know in a straightforward way whether one is using a set of domain parameters susceptible to the new-discovered attack.

Some may say that what one cares about cracking an ECC private key, and not the domain parameters. This means that any algorithm, which computes logarithms using one particular generator, can be used as a subroutine to compute logarithms using any other generator. As the generator for ECC has prime order, this means any ECC public key is also a generator. Therefore, breaking one ECC public key implies the ability to break all ECC public keys using the same set of domain parameters. This implies that either all ECC public keys from a specific set of domain parameters can be broken or none can be, there is no special strength or weakness about any particular (valid) public key and any apparent structure in the associated private key that might hypothetically allow an attack is an illusion.

Another way to view this is that the specific value for a private key depends on the generator, using a different generator results in an entirely different value for the private key, that is, the specific value for a private key is arbitrary. This means that the code for ECC key pair generation does not need to change when an attack is discovered only the input domain parameters need to change.
If a weak set of domain parameters is found, it can be revoked (along with all its associated public keys) and replaced with either an existing strong set or a new strong set of domain parameters. A cryptosystem can be designed for the possibility of the future discovery of an attack by including the capability in the system for using different sets of domain parameters. That is, ECC systems can be designed so they are future resilient to the discovery of new special-purpose attacks.

Further, in future, this work can be implemented in FPGA for real time applications. Then the chip can be fabricated for this system. The common threats in the software based ECC algorithm like overflow buffer, randomness, directory harvest attacks will not affect the hardware based ECC cryptographic system. Thus in the proposed hardware ECC cryptographic system the security level can be further increased than the software system.