Chapter 9
Conclusions and Future Work

9.1 Conclusions: The major conclusions drawn from the results available for MATLAB, DSP and VLSI implementations are as follows:

(i) DSP implementation of security algorithms is highly attractive option due to flexibility, good speed performance and code tuning facility for improvement in efficiency.

(ii) DSP is already used for many applications in mobile communications and adding one more functionality of encryption into it will be desirable.

(iii) VLSI implementation gives very good throughput but this speed is not required for 3G data rates and hence we prefer and recommend DSP implementations in RNC and UE. The mandatory requirements for hardware implementation by some countries will require specialized encryption chips for this purpose.

(iv) MATLAB implementation allows us to build SIMULINK blocks .This can be linked to Code Composer Studio and VLSI synthesis tools if library support is available in SIMULINK. System level simulation is possible with encryption features included in performance analysis.

(v) MATLAB implementation of AES shows that maximum time is spent in initialization, S-box generation, finding inverse of matrices and polynomial multiplications.

(vi) MATLAB implementation of f8 shows that maximum time is spent by KASUMI, fo and fi functions. It is also found that f8 is ten times faster than AES on general purpose processor.

(vii) DSP emulator analysis shows that both f8 and f9 algorithms give almost same performance in speed .

(viii) The fastest algorithm on DSP platform is a set of MILENAGE functions .

(ix) DSP simulator analysis shows that 43% increase in f8 speed requires 21% increase in memory.

(x) DSP simulator analysis shows that 37% increase in f9 speed requires 25% increase in memory.

(xi) DSP simulator analysis for MILENAGE shows that doubling the memory size increases the speed of execution by a factor of four.

(xii) DSP simulator analysis of IDEA indicates that increasing memory size by a factor of 1.2 leads to speed increase by a factor of 2.15.

(xiii) Message length increase reduces encryption speed for f8 algorithm .Five times larger message length means 4.46 times reduced speed on DSP platform .

(xiv) Message length increase reduces the speed of f9 algorithm. If we increase message length by a factor of five, DSP encryption slows down by a factor of 3.25.

(xv) Both f8 and f9 functions give almost same through put on VLSI platform.

(xvi) KASUMI as a core algorithm is almost ten times faster than f8 and f9 algorithms on VLSI platform whereas on DSP platform, all three algorithms run with same speed.

9.2 Future Work: The work carried out by us can be further extended to enhance 3G security features in the following ways:

(i) The algorithms can be embedded inside DSP core architecture with additional cryptographic instruction set taking care of security features. This will enhance the speed and security both and simultaneously providing flexibility.

(ii) The complete cryptography toolbox can be designed as an integral part of MATLAB and SIMULINK. This will be very useful to study cryptography as an essential feature for wireless security.

(iii) Simulation of end-to-end encryption and link-by-link encryption can be taken up once encryption and decryption functions are designed as SIMULINK blocks. These blocks can be designed for all major algorithms and can be simultaneously integrated with communication protocols.

(iv) Profiling of all algorithms on DSP platform has been done. The functions consuming maximum amount of execution time/requiring maximum memory size can be modified without seriously affecting cryptographic strength of the algorithms.