### List of Figures

1.1 Structure of the IMSI. ........................................... 2

2.1 Basic architecture of a mobile system. .......................... 13
2.2 Existing trust model. ............................................. 14
2.3 Proposed trust model. ............................................. 16

3.1 Security architecture of UMTS. .................................. 21
3.2 Generation of AV. .................................................. 23
3.3 Content of AV. ..................................................... 24
3.4 UMTS authentication and key agreement. ......................... 25
3.5 Transmission of IMSI in clear text. .............................. 27
3.6 Home network's database with RIC-Index. ....................... 31
3.7 Protocol flow of UMTS-AKA-with-E2EUIC. ....................... 35
3.8 Generation of $A_{pos}$ and $A_{XOR}$. .......................... 47
3.9 Embedding of $RIC$ into $RAND$. ............................... 48
3.10 P-value plot. ..................................................... 55

4.1 Simplified security architecture of LTE. ......................... 59
4.2 Key hierarchy. .................................................... 63

5.1 Simplified roaming security architecture of 3GPP-WLAN. .... 76
5.2 Simplified roaming security architecture of Non3GPP-EPS. .... 78
5.3 Temporary identity generation. ................................... 81
List of Figures

5.4  HSS's database for EAP-AKA-with-E2EUCIC .......................... 88
5.5  Flow of instructions at the HSS ........................................... 91

6.1  Deduction of security goals ............................................. 100

A.1  Simplified roaming security architecture for access to IP services
     provided by HPLMN in 3GPP-WLAN .................................... 146

B.1  Simplified roaming security architecture for access to IP services
     provided by HPLMN in Non3GPP-EPS ................................. 148